

С. Б. ГАШКОВ

СОВРЕМЕННАЯ ЭЛЕМЕНТАРНАЯ АЛГЕБРА

В ЗАДАЧАХ И УПРАЖНЕНИЯХ

Москва
Издательство МЦНМО
2006

УДК 512
ББК 22.141я721.6
Г12

Гашков С.Б.

Г12 Современная элементарная алгебра в задачах и решениях. —
М.: МЦНМО, 2006. — 328 с.
ISBN 5-94057-211-1

Эта книга представляет собой учебное пособие по алгебре для учащихся 10–11 классов математических школ, содержащее многочисленные задачи и упражнения. Её основу составили лекции, читавшиеся автором в ФМШ МГУ.

Книга может представлять интерес также для преподавателей математики, студентов и для всех интересующихся математикой.

ББК 22.141я721.6

Редакторы: Устинов А.В., Коробкова Т.Л.

Сергей Борисович Гашков

Современная элементарная алгебра в задачах и упражнениях.

Подписано в печать 15.11.2005 г. Формат 60 × 90 ¹/₁₆. Бумага офсетная.
Печать офсетная. Печ. л. 20,5. Тираж 2000 экз. Заказ № .

Издательство Московского центра
непрерывного математического образования
119002, Москва, Большой Власьевский пер., 11. Тел. 241-74-83.

ООО «М-Пресс». 610033, г. Киров, ул. Московская, 122.

Отпечатано в полном соответствии с качеством предоставленных диапозитивов
в ОАО «Дом Печати—ВЯТКА». 610033, г. Киров, ул. Московская, 122.

Книги издательства МЦНМО можно приобрести в магазине «Математическая книга»,
Большой Власьевский пер., д. 11. Тел. 241-72-85. E-mail: biblio@mcme.ru

ISBN 5-94057-211-1

© Гашков С. Б., 2006
© МЦНМО, 2006

Предисловие

Предлагаемая вниманию читателя книга представляет собой учебное пособие по алгебре для учащихся 10-х и 11-х классов физико-математических школ. Его основу составили записи лекций, читавшихся автором в специализированном учебно-научном центре МГУ им. М. В. Ломоносова — школе имени академика А. Н. Колмогорова, более известной под названиями ФМШ МГУ и интернат МГУ. Книга покрывает курс алгебры для учащихся 10-х классов СУНЦ (и аналогичных ему учебных заведений) и содержит основную часть обязательного курса алгебры для 11-х классов.

По традиции, установленной А. Н. Колмогоровым, курс алгебры для «ФМШат», который читали в разное время сам А. Н. Колмогоров, В. И. Арнольд, В. М. Алексеев, Н. Б. Алфутова, В. В. Вавилов, О. Н. Василенко, И. Б. Гашков, С. Б. Гашков, А. А. Егоров, А. Н. Земляков, В. А. Колосов, Ю. В. Нестеренко, В. Ф. Пахомов, А. А. Русаков, Т. Н. Трушанина, А. В. Устинов, О. А. Чалых, В. Н. Чубариков (приношу свои извинения тем, кого не вспомнил или о ком не знал), состоит из двух частей: некоторого обязательного набора понятий, конструкций и теорем (эта часть является общей для всех лекционных курсов алгебры, читавшихся в этой школе) и решения некоторой интересной содержательной проблемы (например, построение циркулем и линейкой правильных n -угольников, теорема Абеля—Руффини о неразрешимости в радикалах общего уравнения пятой степени, квадратичный закон взаимности и т. п.). Вторую часть курса лектор определяет в соответствии со своими вкусами.

В этой книге излагается первая часть курса, а также некоторый вариант дополнительных глав. В ней много задач, в основном довольно трудных.

Она может служить учебным пособием по алгебре и для студентов вузов.

Автор выражает глубокую благодарность В. А. Колосову, материалы которого существенно использовались при подготовке книги, а также А. В. Устинову за тщательное редактирование.

Автор приносит извинения за оставшиеся в книге неточности и небрежности и за то, что не успел подготовить ее к 40-летию ФМШ МГУ и 100-летию А. Н. Колмогорова.

Глава I. Числа и комбинаторика

§ 1.1. Позиционные системы счисления

Еще средневековые математики Ближнего Востока нашли простой подход к вычислениям с дробными числами — использование десятичных позиционных дробей. Позиционная десятичная система попала туда, видимо, из Индии, хотя позиционные дроби, правда не десятичные, а шестидесятеричные, были известны еще в Древнем Шумере, а десятичные дроби по существу были известны в Древнем Китае. Отметим еще, что двадцатеричную систему знали индейцы майя. Здесь уместно напомнить читателю, что запись

$$(a_n \dots a_0, a_{-1} \dots a_{-k})_b$$

в позиционной b -ичной системе означает число, равное

$$a_n b^n + \dots + a_1 b + a_0 + a_{-1} b^{-1} + \dots + a_{-k} b^{-k},$$

где

$$a_n b^n + \dots + a_1 b + a_0$$

— его целая, а

$$a_{-1} b^{-1} + \dots + a_{-k} b^{-k}$$

— дробная часть. В западных странах вместо запятой, отделяющей целую часть от дробной, используется точка.

Почему обычно используется десятичная система? Главным образом, в силу традиции (которая, вероятно, основывается на том, что число пальцев на обеих руках равно обычно 10; индейцы майя, возможно, не забыли и про ноги). Как писал Паскаль *, десятичная система ничем не лучше систем с другими основаниями. Более того, с некоторых точек зрения удобнее другие системы. Так, много поклонников имеет двенадцатеричная система (идущая от счета дюжинами и grosсами — дюжинами дюжин). Возможно, к их числу относился и Г. Дж. Уэллс (см. его роман «Когда спящий проснется»). Преимущество этой системы в том, что 12 имеет больше делителей, чем 10, что несколько упрощает деление.

* Б. Паскаль (Blaise Pascal, 1623—1662) — знаменитый французский математик, физик, религиозный философ и писатель.

С этой точки зрения еще лучше шестидесятеричная система (но таблица умножения в этой системе вгоняет в дрожь). Остатки от былого распространения этой системы видны в картографии и астрономии, а алгоритм перевода из этой системы в десятичную запаян в любом калькуляторе для научных расчетов (речь идет о переводе из градусной меры в десятичную и обратно). Кстати, первая запись дробного числа в позиционной системе в Европе была сделана в XIII в. знаменитым Фибоначчи: корень уравнения $x^3 + 2x^2 + 10x = 20$ он нашел в виде $1^\circ 26' 7'' 42'''$.

Есть поклонники и у восьмеричной и шестнадцатеричной систем. Первую из них хотел вести в Швеции Карл XII (который, возможно, пришел к этой идее самостоятельно), но ряд обстоятельств помешали этому прогрессивному начинанию (среди них, вероятно, и занятость короля в военных компаниях, в частности, под Полтавой в России). Преимущество этих систем в том, что легко осуществляется перевод в двоичную систему и обратно.

Двоичная система в каком-то смысле была известна в Древнем Китае. В классической книге «И цзин» («Книга перемен») приведены диаграммы, так называемые Фу-си, первая из которых имеет вид , а последняя (шестдесят четвертая) — вид  (нулям и единицам соответствуют сплошные и прерывистые линии). Китайцы не поленились придумать для этих диаграмм специальные иероглифы и названия.

Возможно, что идея двоичной системы была известна и древним индийцам. Об этом, например, говорит известная легенда об изобретателе шахмат, который скромно попросил (после настояний магараджи, которому очень понравилась игра) себе в награду положить одно зерно на угловую клетку шахматной доски и удваивать количество зерен на каждой следующей клетке.

В Европе двоичная система, видимо, появилась уже в новое время. Об этом свидетельствует система объемных мер, применяемая английскими виноторговцами: два джилла = полуштоф, два полуштофа = пинта, две пинты = кварта, два кварта = потл, два потла = галлон, два галлона = пек, два пека = полубушель, два полубушеля = бушель, два бушеля = килдеркин, два килдеркина = баррель, два барреля = хогзхед, два хогзхеда = пайп, два пайпа = тан.

Читатели исторических романов знакомы с пинтами и квартами. Частично эта система дожила и до нашего времени (нефть и бензин до сих пор меряют галлонами и баррелями). Удобство двоичной системы при взвешивании демонстрируют также помещенные в конце параграфа задачи, вторая из которых заимствована из материалов жюри международных олимпиад, а третья известна, вероятно, со средневековых времен.

Пропагандистом двоичной системы был знаменитый Г. В. Лейбниц * (получивший от Петра I звание тайного советника). Он отмечал особую простоту алгоритмов арифметических действий в двоичной арифметике в сравнении с другими системами и придавал ей определенный философский смысл. Говорят, что по его предложению была выбита медаль с надписью «Для того, чтобы вывести из ничтожества все, достаточно единицы».

Известный современный математик Д. Данциг ** о нынешнем положении дел сказал: «Увы! То, что некогда возвышалось как монумент монотеизму, очутилось в чреве компьютера». Причина такой метаморфозы — не только уникальная простота таблицы умножения в двоичной системе, но и особенности физических принципов, на основе которых работает элементная база современных ЭВМ (за последние 40 лет она неоднократно менялась, но двоичная система и булева алгебра по-прежнему вне конкуренции).

Отметим еще, что двоичная система находит применения и в других математических задачах, например при анализе известной игры «Ним». Игра состоит в следующем: на столе лежит несколько кучек спичек, и два игрока по очереди выбирают одну из кучек и забирают из нее сколько угодно спичек (хоть все); проигрывает тот, кто забирает последнюю. Эпизод с этой игрой неоднократно повторяется в известном французском фильме «Прошлым летом в Мариенбаде».

Упомянутая стратегия поддается для реализации даже на специализированных машинах. Одна из таких машин была выставлена после войны в Берлине на английской выставке и с успехом конкурировала с находящимся рядом бесплатным пивным залом. Известный популяризатор математики Мартин Гарднер в одной из своих книг пишет, что Алан Тьюринг *** вспоминал о том, как популярность этой машины повысилась еще больше после победы над тогдашним бундесминистром экономики Л. Эрхардом.

Некоторую конкуренцию двоичной системе как по простоте арифметических алгоритмов, так и по количеству применений в математических задачах может составить троичная система, в частности ее вариант, называемый уравновешенной троичной системой, в которой вместо цифры 2 используется цифра -1 .

* Г. В. Лейбниц (Gottfried Wilhelm Leibniz, 1646—1716) — великий немецкий математик и философ, один из основоположников математического анализа.

** Д. ван Данциг (David van Danzig, 1900—1959) — голландский математик, изобретатель симплекс-метода в линейном программировании.

*** А. Тьюринг (Alan Mathison Turing, 1912—1954) — английский математик, один из создателей теории алгоритмов. При его участии был построен первый английский компьютер.

Представление о ней дает следующая в конце параграфа задача 6, опубликованная в книге Баше де Мезириака * в XVII в.

Троичная система применяется при объяснении следующего фокуса Жергонна **. Зритель запоминает одну из 27 карт и выкладывает их в три стопки по 9 карт картинками вверх (первая карта идет в первую стопку, вторая — во вторую, третья — в третью, четвертая — в первую и т. д.). Фокуснику сообщается, в какой из стопок задуманная карта, потом стопки складываются в любом из шести возможных порядков (не перетасовывая карты внутри стопок) и раскладываются снова в три стопки, начиная с верхней карты, потом складываются опять и процедура повторяется в третий раз (каждый раз сообщается, в какую из стопок легла запомненная карта). Фокусник каждый раз замечает, куда легла стопка с запомненной картой — сверху (это отмечается в уме символом 0), в середину (символ 1), или в низ колоды (символ 2), и составляет из этих символов трехзначное число в троичной системе счисления, ставя первый из замеченных символов в младший разряд, следующий символ — во второй и последний символ — в старший разряд. К полученному числу прибавляется единица и отсчитывается столько карт, начиная с верхней карты колоды — последняя из отсчитанных карт и есть запомненная зрителем.

Имеется еще один вариант фокуса Жергонна, но с другим способом раскладки карт. Колода из 27 карт раскладывается в три стопки в следующем порядке: первая карта — в первую стопку, вторая — во вторую, третья — в третью, четвертая — опять в третью, пятая — во вторую, шестая — в первую и т. д. Одна из карт запоминается зрителем и указывается стопка, в которой она лежит, и все повторяется еще два раза. Способ угадывания тот же самый. Можно показывать тот же фокус и с 21 картой, но тогда надо раскладывать карты самому и стопку с задуманной картой всегда класть в середину колоды.

Уравновешенная система может быть рассмотрена и для любого натурального основания, правда, при четном основании запись в ней перестает быть однозначной. Преимуществом уравновешенных систем является то, что в них записываются и отрицательные числа без знака минус перед записью, а также то, что таблица умножения в этих системах в сравнении с обычными примерно в четыре раза короче, как отметил О. Л. Коши ***.

* Баше де Мезириак (Gaspard Claude Bachet de Mésiriac, 1587–1638) — французский математик и поэт, автор одной из первых книг по занимательной математике.

** Ж. Жергонн (Josef Diaz Gergonne, 1771–1859) — французский математик, член-корреспондент Парижской академии наук.

*** О. Л. Коши (Augustin Louis Cauchy, 1789–1857) — великий французский математик, член Петербургской академии наук. По политическим взглядам ультрароялист, сторонник Бурбонов, клерикал. Восемь лет провел в эмиграции.

Можно рассматривать системы счисления и с отрицательным основанием b , но неотрицательными цифрами $0, 1, \dots, -b - 1$. Любое целое число можно представить в этой системе без знака.

Основатель теории множеств Георг Кантор* предложил рассматривать системы счисления со смешанными основаниями. Запись в таких системах выглядит так:

$$\begin{aligned} \dots a_3, a_2, a_1, a_0; a_{-1}, a_{-2}, a_{-3}, \dots, \\ \dots b_2, b_1, b_0; b_{-1}, b_{-2}, b_{-3}, \dots, \end{aligned}$$

где b_i — основания, a_i — цифры, $0 \leq a_i < b_i$, и расшифровывается следующим образом:

$$\dots a_3 b_2 b_1 b_0 + a_2 b_1 b_0 + a_1 b_0 + a_0 + a_{-1}/b_{-1} + a_{-2}/(b_{-2} \cdot b_{-1}) + \dots$$

Частным случаем таких систем является факториальная, которая получается при $b_k = k + 2$, $b_{-k} = k + 1$. Используя ее, можно любое натуральное число представить в виде

$$a_{n-1}n! + \dots + a_1 2! + a_0 1!,$$

где $0 \leq a_k \leq k + 1$.

Системы со смешанными основаниями всем известны из повседневной жизни. Например, «1 неделя, 2 дня, 3 часа, 4 минуты, 56 секунд, 789 миллисекунд» равно

$$\begin{array}{cccccc} 1, & 2, & 3, & 4, & 56; & 789; \\ & & 7, & 24, & 60, & 60; & 1000 \end{array}$$

секунд.

И, наконец, вернемся к обычной позиционной системе и рассмотрим вопрос о представлении отрицательных чисел в ЭВМ. Обычный способ записи отрицательных чисел состоит в постановке знака минус перед записью модуля этого числа. Этот способ называется прямым кодом. Для ЭВМ, как правило, удобнее дополнительный код, когда, например, число $-(123456789)_{10}$ записывается как

$$10^9 - (123456789)_{10} = (876543211)_{10}.$$

При этом операции сложения-вычитания фактически проводятся по модулю 10^9 и не возникает проблемы «минус нуля». Дополнительный код удобен еще и тем, что при вычитании из меньшего числа большего с помощью обычного алгоритма вычитания как раз и получается разность, записанная в дополнительном коде. Но есть у него и недостатки. Кроме дополнительного кода рассматривают также обратный код, в котором,

* Г. Кантор (Georg Cantor, 1845–1918) — знаменитый немецкий математик. Родился в Санкт-Петербурге.

например, число $-(123456789)_{10}$ записывается как 876543210 (каждая цифра дополняется до 9). В этом коде сложение и вычитание производятся фактически по модулю $10^9 - 1$.

Задачи и упражнения к § 1.1

1. Оцените, сколько тонн зерна придется выплатить магарадже.
- 2*. За какое наименьшее количество взвешиваний на чашечных весах можно отвесить один килограмм сахарного песка, если имеется лишь одна однограммовая гирька?
- 3*. Чтобы взвесить любое число граммов песка от 1 до n граммов за одно взвешивание, достаточно иметь гири весом 1, 2, 4, ..., 2^m граммов, где $m = \lfloor \log_2 n \rfloor$, и меньшего числа гирь недостаточно, если песок лежит на одной чашке весов, а гири разрешается ставить на вторую чашку.
- 4**. Укажите выигрывающую стратегию в игре «Ним».
5. Любое целое число от $-(3^n - 1)/2$ до $(3^n - 1)/2$ может быть однозначно представлено в виде

$$a_{n-1}3^{n-1} + \dots + a_13 + a_0,$$

где цифры $a_i = 0$ или ± 1 .

6*. Допустим, что при взвешивании разрешается класть гири и на чашку весов с грузом. Тогда для того, чтобы взвесить любой груз от 1 до $(3^n - 1)/2$ граммов за одно взвешивание, достаточно иметь гири весом 1, 3, 9, ..., 3^{n-1} граммов, и меньшего количества гирь недостаточно.

7*. Объясните фокус Жергонна.

8*. Докажите, что во втором варианте фокуса Жергонна (с 21 картой) после трех сдач задуманная карта окажется точно в середине колоды, т. е. на одиннадцатом месте от любого края.

9. Запишите число $(1234567890)_{10}$ в уравновешенной десятичной системе счисления.

10. Докажите, что любое ненулевое целое число имеет единственное знакопеременное двоичное представление

$$2^{\alpha_0} - 2^{\alpha_1} + \dots + (-1)^k 2^{\alpha_k},$$

где $\alpha_0 < \dots < \alpha_k$.

11. Представьте в «негадесятичной» системе (т. е. в системе с отрицательным основанием -10) числа

$$(1234567890)_{10}, \quad -(1234567890)_{10}.$$

12*. Запишите в факториальной системе счисления число e — основание натуральных логарифмов.

13. Докажите, что остаток от деления произвольного числа на 9 равен остатку от деления на 9 суммы его цифр в записи по основанию 10. Такой же признак делимости справедлив и для числа 3.

14. Обозначим сумму десятичных цифр числа a через $\nu_{10}(a)$. Найдите

$$\nu_{10}(\nu_{10}(\nu_{10}(4444^{4444}))).$$

Целой частью числа x называется такое целое число $n = \lfloor x \rfloor$, которое удовлетворяет неравенствам $n \leq x < n + 1$. *Дробной частью* числа x называется число $\{x\} = x - \lfloor x \rfloor$. Целое число $m = \lceil x \rceil$ такое, что $m - 1 < x \leq m$, называется *верхней целой частью*. Число

$$\|x\| = \min(x - \lfloor x \rfloor, \lceil x \rceil - x)$$

называется *расстоянием до ближайшего целого* числа, а само это целое число обозначается $((x))$ в случае, если $x \neq n + 1/2$, т. е. не является *полуцелым*. В последнем случае функция $((x))$ естественным образом не определена, но ее можно доопределить, если угодно, например, равенством $((n + 1/2)) = n$. Название для последней функции не является общепринятым, впрочем, общепринятого названия и нет.

Для целой части в последнее время (благодаря книгам Д. Кнута и распространению издательской системы TeX) входит в моду название «пол» и обозначение $\lfloor x \rfloor$, а верхнюю целую часть все чаще называют «потолком» и обозначают $\lceil x \rceil$. В старое время целую часть называли иногда французским термином «антье».

15. Докажите, что функции $\{x\}$, $\|x\|$ периодичны с наименьшим периодом единица и постройте их графики. Проверьте, что

$$\lceil x \rceil = -\lfloor -x \rfloor, \quad ((x)) = \lfloor 2x \rfloor - \lfloor x \rfloor \quad (\text{при } x \text{ не полуцелом}),$$

$$\|x\| = |x - ((x))| \quad (\text{при } x \text{ не полуцелом}),$$

$$\|x\| = \min(\{x\}, 1 - \{x\}) = \frac{1}{2} - \left| \{x\} - \frac{1}{2} \right|.$$

16. Докажите, что $\lfloor x + 1/2 \rfloor = \lfloor 2x \rfloor - \lfloor x \rfloor$, $\lfloor x \rfloor + \lfloor y \rfloor + 1 \geq \lfloor x + y \rfloor \geq \lfloor x \rfloor + \lfloor y \rfloor$, $0 \leq \lfloor 2x \rfloor - 2\lfloor x \rfloor \leq 1$, $\lfloor 2x \rfloor + \lfloor 2y \rfloor \geq \lfloor x \rfloor + \lfloor y \rfloor + \lfloor x + y \rfloor$, $\lceil \lfloor x \rfloor / n \rceil = \lfloor x/n \rfloor$.

17. Докажите, что $\lceil x - 1/2 \rceil = \lceil 2x \rceil - \lceil x \rceil$, $\lceil x \rceil + \lceil y \rceil - 1 \leq \lceil x + y \rceil \leq \lceil x \rceil + \lceil y \rceil$, $0 \leq 2\lceil x \rceil - \lceil 2x \rceil \leq 1$, $\lceil 2x \rceil + \lceil 2y \rceil \leq \lceil x \rceil + \lceil y \rceil + \lceil x + y \rceil$, $\lceil \lceil x \rceil / n \rceil = \lceil x/n \rceil$.

18. Докажите, что при x не полуцелом

$$((x)) = \left\lceil x + \frac{1}{2} \right\rceil - \left\lceil \frac{2x+1}{4} \right\rceil + \left\lfloor \frac{2x+1}{4} \right\rfloor.$$

19. Выразить количество целых чисел, находящихся на промежутке

а) $(a, b]$ (т. е. удовлетворяющих неравенствам $a < x \leq b$);

б) (a, b) (т. е. удовлетворяющих неравенствам $a < x < b$),

через функции «пол» и «потолок».

20. (Мак-Элис.) Пусть $f(x)$ — непрерывная строго возрастающая на отрезке I функция. Если x лежит в I , то $\lfloor x \rfloor$ и $\lceil x \rceil$ тоже лежат в этом отрезке.

Тогда равенства

$$\lfloor f(\lfloor x \rfloor) \rfloor = \lfloor f(x) \rfloor \quad \text{и} \quad \lceil f(\lceil x \rceil) \rceil = \lceil f(x) \rceil$$

равносильны друг другу и выполняются тогда и только тогда, когда функция обладает следующим свойством: если $f(x)$ — целое число, то и x — тоже целое число.

21. Докажите, что $\lfloor \sqrt{n(n+1)(n+2)(n+3)} \rfloor = n^2 + 3n$.

22*. (В. Тебо.) Докажите, что

$$\lfloor \sqrt[4]{n(n+1) \dots (n+7)} \rfloor = n^2 + 7n + 6.$$

В дальнейшем будем использовать следующие стандартные обозначения: $\mathbb{N}$ — множество натуральных чисел, $\mathbb{Z}$ — множество целых чисел, $\mathbb{P}$ — множество простых чисел, $\mathbb{Q}$ — множество рациональных чисел, $\mathbb{R}$ — множество действительных чисел, $\mathbb{C}$ — множество комплексных чисел (о последних пойдет речь в § 4.3).

§ 1.2. Натуральные числа

Определение 1. Если a — целое число, b — натуральное число, то *неполным частным* q и *остатком* r от деления числа a на число b называются такие целые числа, что

$$a = bq + r \quad \text{и} \quad 0 \leq r < b.$$

Теорема 1. Для любого целого числа a и натурального числа b неполное частное и остаток от деления a на b существуют и определены однозначно.

Доказательство. Существование неполного частного и остатка очевидно (на самом деле не совсем очевидно, но мы в такие тонкости вдаваться здесь не будем).

Единственность доказывается от противного. Допустим, что существуют два разложения: $a = bq_1 + r_1 = bq_2 + r_2$. Тогда $0 < |r_1 - r_2| < b$ и в то же время $|r_1 - r_2| = b \cdot |q_1 - q_2| \geq b$. $\square$

Определение 2. Если $r = 0$, то пишем $b \mid a$ и говорим, что b — *делитель* a (или что a делится на b).

Любое натуральное число n имеет два так называемых *несобственных делителя* 1 и n (число $n = 1$ имеет один делитель). Остальные делители числа n называются *собственными*.

Определение 3. Если число, большее единицы, не имеет собственных делителей, то оно называется *простым*.

Число, имеющее собственные делители, называется *составным*.

Единица — особое число. Оно не причисляется ни к тем, ни к другим.

Принципом наименьшего числа называется следующее утверждение: *любое непустое множество натуральных чисел содержит наименьшее число*.

Этот принцип эквивалентен различным вариантам принципа математической индукции (далее просто индукции), например такому: если A — множество натуральных чисел, содержащее единицу (это предположение соответствует так называемой *базе индукции*), и вместе с каждым числом n содержащее следующее за ним число $n + 1$ (это предположение соответствует так называемому *шагу индукции*), то множество A совпадает с множеством всех натуральных чисел $\mathbb{N}$. Принцип индукции далее мы принимаем за аксиому.

Укажем ряд его применений.

Теорема 2. *Любое натуральное число, большее единицы, разлагается в произведение простых чисел.*

Доказательство. Обозначим через A множество всех таких натуральных чисел n , что число $n + 1$ разлагается на простые множители. Очевидно, что 1 принадлежит множеству A — *база индукции* проверена. Докажем, что можно сделать *шаг индукции*. Пусть множество $\{1, \dots, n\}$ содержится в множестве A . Проверим, что $n + 1$ содержится в A . Если $n + 1$ — простое число, то это очевидно. Если $n + 1$ не простое, то $n + 1 = a \cdot b$, где a, b — натуральные числа, $1 < a, b \leq n$. Так как числа a, b принадлежат множеству A , то $a = p_1 \cdot p_2 \cdot \dots \cdot p_s$, $b = p_{s+1} \cdot p_{s+2} \cdot \dots \cdot p_m$, где $p_i, i = 1, \dots, m$, — простые числа. Тогда число $n + 1 = a \cdot b = p_1 \cdot p_2 \cdot \dots \cdot p_m$ тоже принадлежит множеству A . Шаг индукции сделан. Согласно принципу индукции, $A = \mathbb{N}$ и, следовательно, теорема доказана. $\square$

Теорема 3 (Евклид *). *Простых чисел бесконечно много.*

* Евклид Александрийский (Εὐκλείδης, ок. 325–265 до н. э.) — античный математик, автор знаменитого трактата «Начала», бывшего всеобщим учебником математики на протяжении многих столетий. Теорема 3 соответствует предложению 20 из IX книги «Начал».

Доказательство. Предположим противное, а именно, что простых чисел — конечное количество, и $p_1, p_2, \dots, p_n$ — все такие числа. Тогда число $p_1 \cdot p_2 \cdot \dots \cdot p_n + 1$ не делится ни на одно из этих чисел, и поэтому согласно теореме 3 имеет простой делитель, отличный от любого из чисел $p_i, i = 1, \dots, n$. Противоречие. $\square$

Теорема 4 (Гаусс *). *Любое натуральное число $n > 1$ можно единственным способом представить в виде $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$, где α_i — натуральные числа, а $p_1, p_2, \dots, p_n$ — некоторая монотонно возрастающая последовательность простых чисел.*

Доказательство. Существование указанного в формулировке теоремы разложения

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_m^{\alpha_m}, \quad p_1 < p_2 < \dots < p_m$$

(называемого далее *каноническим разложением на простые числа*), следует из теоремы 2. Единственность докажем индукцией по n . База ($n = 2$) очевидна. Индукционный переход обосновывается методом от противного. Пусть числа $2, \dots, n - 1$ однозначно разлагаются на простые, а число n — нет. Можно считать, что число n имеет два различных канонических разложения $n = p_1^{\alpha_1} \cdot \dots \cdot p_m^{\alpha_m} = p_1 \cdot P$ и $n = q_1^{\beta_1} \cdot \dots \cdot q_k^{\beta_k} = q_1 \cdot Q$, и, например, $p_1 \leq q_1$. Ясно, что $Q > 1$, иначе число $q_1 = p_1^{\alpha_1} \cdot \dots \cdot p_m^{\alpha_m}$ не было бы простым, или q_1 было бы равно p_1 , а в этом случае оба разложения бы совпали, чего не может быть.

Рассмотрим все остальные возможные случаи. Если $p_1 = q_1$, то число P равно Q , меньше n и имеет два различных разложения $p_1^{\alpha_1-1} \cdot \dots \cdot p_m^{\alpha_m}$ и $q_1^{\beta_1-1} \cdot \dots \cdot q_k^{\beta_k}$, что ведет к противоречию.

Если же $p_1 < q_1$, то представим число $n - p_1 Q$ в виде $(q_1 - p_1)Q$ и заметим, что оно больше нуля, меньше n и делится на p_1 , так как представимо в виде $p_1(P - Q)$. Но это число имеет два разложения: первое из них получается умножением на p_1 разложения числа $P - Q$, а второе — умножением на Q разложения числа $p_1 - q_1$. Эти разложения различны, так как второе разложение не содержит число p_1 , ведь $p_1 - q_1 < p_1$, а $q_k > \dots > q_1 > p_1$. Полученное противоречие и доказывает теорему. $\square$

Определение 4. *Наибольшим общим делителем* целых чисел a и b называется наибольшее число НОД(a, b), которое делит a и b .

Два числа называются *взаимно простыми*, если их наибольший общий делитель равен единице.

* К. Гаусс (Carl Friedrich Gauss, 1777–1855) — великий немецкий математик, прозванный еще при жизни «королем математиков».

Упражнение 1. Проверьте, что $\text{НОД}(a, b) = \text{НОД}(a - bq, b)$ для любых целых a, b, q .

Определение 5. *Наименьшим общим кратным* целых чисел a и b называется наименьшее число $\text{НОК}(a, b)$, которое делится на оба этих числа.

Для НОД и НОК применяются также краткие обозначения a, b и $[a, b]$.

Теорема 5. *Наибольший общий делитель* $\text{НОД}(a, b)$ выражается через a и b посредством формулы $\text{НОД}(a, b) = ap + bt$, где p, t — целые числа.

Доказательство. Разделим с остатком a на b :

$$a = bq_1 + r_1$$

и заметим, что $\text{НОД}(a, b) = \text{НОД}(b, r_1)$ и числа a, b, r_1 представимы в виде $ap + bt$, где p, t — целые числа. Действительно,

$$a = 1 \cdot a + 0 \cdot b, \quad b = 0 \cdot a + 1 \cdot b,$$

$$r_1 = a - q_1b = n_1a + m_1b, \quad n_1 = 1, \quad m_1 = -q_1.$$

Аналогично разделим b на r_1 :

$$b = r_1q_2 + r_2, \quad \text{НОД}(b, r_1) = \text{НОД}(r_1, r_2)$$

и представим r_2 как

$$b - r_1q_2 = b - q_2(n_1a + m_1b) = -q_2n_1a + (-q_2m_1 + 1)b = n_2a + m_2b,$$

$$n_2 = -q_2n_1, \quad m_2 = -q_2m_1 + 1.$$

Далее разделим r_1 на r_2 :

$$r_1 = r_2q_3 + r_3, \quad \text{НОД}(r_1, r_2) = \text{НОД}(r_2, r_3)$$

и представим r_3 как

$$r_1 - r_2q_3 = n_1a + m_1b - q_3(n_2a + m_2b) = n_3a + m_3b,$$

$$n_3 = n_1 - q_3n_2, \quad m_3 = m_1 - q_3m_2$$

и т. д. Остатки r_i при этом уменьшаются, значит, процедура окончится за конечное число шагов:

$$r_{k-1} = r_kq_{k+1} + r_{k+1}, \quad r_{k+1} \mid r_k, \quad r_k = r_{k+1}q_{k+2}.$$

Заметим, что $r_{k+1} = \text{НОД}(a, b)$, так как $\text{НОД}(r_k, r_{k+1}) = r_{k+1}$, и

$$d = \text{НОД}(a, b) = r_{k+1} = n_{k+1}a + m_{k+1}b = na + mb.$$

□

Общее число арифметических операций, затраченных на вычисление НОД(a, b), равно $k + 2$, и еще $4k + 3$ операции нужны для нахождения коэффициентов n, m , называемых иногда *коэффициентами Безу**.

Метод, с помощью которого только что был найден наибольший общий делитель, называется алгоритмом Евклида, точнее, *расширенным алгоритмом Евклида*, так как обычный алгоритм Евклида не вычисляет коэффициентов Безу. Это едва ли не самый известный алгоритм в математике (дедушка всех алгоритмов, по словам Дональда Кнута).

В качестве приложения доказанной теоремы получим следующую лемму.

Лемма 1. (i) Если целые числа a и b взаимно просты и a делит произведение b на целое число c , то a делит c .

(ii) Если произведение $a_1 \dots a_m$ делится на простое число p , то хотя бы один из его сомножителей a_i делится на p .

Доказательство. Докажем первое утверждение. Из предыдущей теоремы следует, что

$$an + bm = 1.$$

Умножив обе части этого равенства на c , получим равенство

$$acn + bmc = c.$$

Очевидно, что $a \mid acn$, $a \mid bc$, значит, $a \mid bcm$ и $a \mid acn + bmc = c$.

Второе утверждение выведем из первого. Можно предположить, что a_i не делится на p при всех $i < m$ (иначе нечего доказывать). Так как p — простое, то это означает взаимную простоту p с любым числом a_i , $i < m$. Применяя $m - 1$ раз первое утверждение леммы, получаем, что a_m делится на p . $\square$

З а м е ч а н и е 1. Эту лемму легко также доказать с помощью только что доказанной теоремы Гаусса об однозначности разложения на простые множители (называемой иногда основной теоремой арифметики). Однако не принято выводить легкие теоремы из трудных, и мы, опираясь на упомянутую лемму, получим другое доказательство теоремы Гаусса (быть может, более простое, чем приведенное раньше) также методом математической индукции.

Предположим, что мы доказали теорему для всех чисел, меньших n . Пусть $n = q_1^{\alpha_1} \cdot q_2^{\alpha_2} \cdot \dots \cdot q_t^{\alpha_t}$ — каноническое разложение на простые множители. Докажем, что это разложение единственно.

* Э. Безу (Etienne Bezout, 1730–1783) — французский математик, член Парижской академии наук.

Предположим противное, а именно, что существует иное каноническое разложение n на простые множители: $n = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \dots \cdot p_s^{\beta_s}$. Можно предположить (как говорят, без ограничения общности) также, что $p_1 \geq q_1$. Так как q_1 делит n , то согласно лемме 1 число q_1 делит некоторое число p_i , а значит, $q_1 = p_i$ (в силу простоты этих чисел). Ввиду монотонной упорядоченности последовательности p_i и неравенства $p_1 \geq q_1$ это возможно лишь при $p_1 = q_1$. Отсюда следует, что

$$q_1^{\alpha_1-1} \cdot q_2^{\alpha_2} \cdot \dots \cdot q_t^{\alpha_t} = n/q_1 = n/p_1 = p_1^{\beta_1-1} \cdot p_2^{\beta_2} \cdot \dots \cdot p_s^{\beta_s},$$

и поэтому согласно предположению индукции эти разложения совпадают. Значит, совпадают и исходные разложения $q_1^{\alpha_1} \cdot \dots \cdot q_t^{\alpha_t}$ и $p_1^{\beta_1} \cdot \dots \cdot p_s^{\beta_s}$, что ведет к противоречию.

Сделаем еще несколько замечаний к алгоритму Евклида.

З а м е ч а н и е 2. Последовательность коэффициентов $m_1, \dots, m_k$ можно не вычислять, сэкономив таким образом $2k-2$ операции, так как нужный нам коэффициент $m = m_{k+1}$ можно найти из равенства $na + mb = \text{НОД}(a, b)$ с помощью всего лишь трех дополнительных операций.

З а м е ч а н и е 3. Так как $n_1m_2 - n_2m_1 = q_2q_1 + 1 - q_2q_1 = 1$,

$$n_{i+1} = n_{i-1} - q_{i+1}n_i, \quad m_{i+1} = m_{i-1} - q_{i+1}m_i,$$

выводим по индукции, что

$$\begin{aligned} n_im_{i+1} - n_{i+1}m_i &= (m_{i-1} - q_{i+1}m_i)n_i - (n_{i-1} - q_{i+1}n_i)m_i = \\ &= m_{i-1}n_i - n_{i-1}m_i = (-1)^{i+1}, \end{aligned}$$

откуда следует, что всегда $\text{НОД}(n_i, m_i) = 1$.

По индукции также легко проверить, что последовательности n_i и m_i обе знакопеременные и строго возрастающие по абсолютной величине.

З а м е ч а н и е 4. Если выполнить еще один шаг алгоритма $r_k = r_{k+1}q_{k+2}$, то получим

$$r_{k+2} = 0 = Na + Mb, \quad N = n_k - q_{k+2}n, \quad M = m_k - q_{k+2}m,$$

и так как $\text{НОД}(N, M) = 1$, $\text{НОД}(a/d, b/d) = 1$, значит, число $Na = -Mb$ делится и на a , и на b , а так как $Na/d = -Mb/d$, то N кратно b/d и b/d кратно N , откуда $N = \pm b/d$, и аналогично $M = \pm a/d$, значит, $Na = -Mb = \pm ab/d = \pm \text{НОК}(a, b)$. Таким образом, расширенный алгоритм Евклида вычисляет также и наименьшее общее кратное, а коэффициенты Безу удовлетворяют неравенствам

$$|n| \leq b/\text{НОД}(a, b), \quad |m| \leq a/\text{НОД}(a, b).$$

Задачи и упражнения к § 1.2

1. Дайте подробное обоснование рассуждений из замечаний в конце доказательства теоремы 5.

Иногда *коэффициентами Безу* называют любые целые m, n , для которых $(a, b) = na + mb$.

2*. Докажите существование коэффициентов Безу без использования алгоритма Евклида.

3. Коэффициенты Безу определены неоднозначно. Укажите способ, как по известной паре коэффициентов Безу найдите все остальные такие пары.

Задача поиска коэффициентов Безу — это не что иное, как задача о решении линейного уравнения с двумя неизвестными в целых числах.

4*. Докажите, что существуют коэффициенты Безу, удовлетворяющие или неравенству $|n| \leq b/2 \cdot (a, b)$, или неравенству $|m| \leq a/2 \cdot (a, b)$.

5. Выведите из теоремы 5 следующие утверждения:

а) если $|a_i| = p_1^{\alpha_{i1}} \cdots p_m^{\alpha_{im}}$, $\alpha_{ij} \geq 0$, $i = 1, \dots, n$, $j = 1, \dots, m$, то

$$(a_1, \dots, a_n) = p_1^{\beta_1} \cdots p_m^{\beta_m}, \quad [a_1, \dots, a_n] = p_1^{\gamma_1} \cdots p_m^{\gamma_m},$$

где $\beta_j = \min_i \{\alpha_{ij}\}$, $\gamma_j = \max_i \{\alpha_{ij}\}$;

б) $[a, b] \cdot (a, b) = a \cdot b$;

в) если $c \mid ab$ и $(c, a) = 1$, то $c \mid b$;

г) если $(a, b) = 1$, то уравнение $ax + by = 1$ разрешимо в целых числах;

д) уравнение $a_1x_1 + \dots + a_nx_n = b$ разрешимо в целых числах тогда и только тогда, когда $(a_1, \dots, a_n)$ делит b ;

е) если k — общий делитель a и b , то $(a, b) = k \left(\frac{a}{k}, \frac{b}{k} \right)$.

6. Докажите, что остаток от деления произвольного числа на 99 равен остатку от деления на 99 суммы его цифр в записи по основанию 100. Такой же признак делимости справедлив и для числа 33.

Например, остаток от деления числа 1111111 на 33 равен остатку от деления числа $1 + 11 + 11 + 11 = 34$ на 33, т. е. 1.

7. Докажите, что остаток от деления произвольного числа на 37 равен остатку от деления на 37 суммы его цифр в записи по основанию 1000.

Например, остаток от деления числа 1111111 на 37 равен остатку от деления числа $1 + 111 + 111 = 223$ на 37, т. е. 1.

8. Каким днем недели будет 1 января 2101 года?

9. Докажите, что остаток от деления произвольного числа на 11 равен остатку от деления на 11 знакопеременной суммы его цифр в десятичной записи, в которой число единиц берется со знаком плюс.

Например, остаток от деления числа 1111111 на 11 равен остатку от деления числа $1 - 1 + 1 - 1 + 1 - 1 + 1 = 1$ на 11, т. е. опять 1.

10. Докажите, что остаток от деления произвольного числа на 101 равен остатку от деления на 101 знакопеременной суммы его цифр в записи по основанию 100. Докажите аналогичный признак делимости на 7 и 13.

Приведенные выше признаки делимости являются наиболее часто применяемыми частными случаями *признака делимости Паскаля*.

11. Найдите остатки от деления числа, записываемого 43 единицами, на 3, 7, 11, 13, 37.

12. Найдите остатки от деления числа, записываемого 1 111 111 единицами, на 3, 7, 9, 11, 13, 37.

13. Найдите остаток от деления числа 4444^{4444} на 99.

Обозначим через $a \bmod m$ остаток от деления a на m .

14. Докажите, что $a \bmod m = a - m[a/m]$.

15. (Корректность определения модулярных операций.) Докажите, что для любых целых a, b

$$\begin{aligned} ((a \bmod n) + (b \bmod n)) \bmod n &= (a + b) \bmod n, \\ (a \bmod n)(b \bmod n) \bmod n &= ab \bmod n. \end{aligned}$$

16. (Сочетательный закон для модулярных операций.) Докажите, что для любых целых a, b, c

$$\begin{aligned} ((a + b) \bmod n + c \bmod n) \bmod n &= (a + b + c) \bmod n, \\ (ab \bmod n)(c \bmod n) \bmod n &= abc \bmod n. \end{aligned}$$

17. (Модулярное вычитание.) Докажите, что для любых целых a, b

$$\begin{aligned} ((a \bmod n) - (b \bmod n)) \bmod n &= (a - b) \bmod n, \\ ((a - b) \bmod n + (b \bmod n)) \bmod n &= a \bmod n. \end{aligned}$$

18. (Формула Гаусса для пасхалии.) Для вычисления даты Пасхи в N -м году надо сделать следующие вычисления:

$$\begin{aligned} a &= N \bmod 19, & b &= N \bmod 4, & c &= N \bmod 7, & m &= 15, & n &= 6, \\ d &= (19a + m) \bmod 30, & e &= (2b + 4c + 6d + n) \bmod 7. \end{aligned}$$

Найдем число $22 + d + e$. Датой Пасхи будет $(22 + d + e)$ -е марта, если это число меньше 31, иначе Пасха будет $(d + e - 9)$ -го апреля.

Когда будет Пасха в следующем учебном году?

19. Докажите, что $p_n < 2^{2^n}$, где $p_n - n$ -е по величине простое число.

20*. Докажите, что простых чисел вида а) $4k - 1$; б) $6k - 1$ бесконечно много.

21*. Докажите, что для любого n найдутся n подряд идущих чисел, среди которых а) нет простых; б) ровно одно простое.

22. Число вида $4k + 1$ назовем *псевдопростым*, если оно не разлагается в произведение чисел такого же вида, отличных от 1. Докажите, что любое число вида $4k + 1$ разлагается в произведение псевдопростых.

Проверить, что число 693 имеет два различных разложения на псевдопростые.

23. Пусть a, n — натуральные числа. Докажите, что если $a^n - 1$ простое, то $a = 2$ и n простое. Проверить, что $2^p - 1$ не всегда будет простым, если p — простое. Простые вида $2^p - 1$ называются *простыми числами Мерсенна* *.

24. Докажите, что если $2^n + 1$ простое, то n — степень двойки.

25. Числа $f_n = 2^{2^n} + 1$ называются *числами Ферма* **. Первые четыре из них — простые, но уже $2^{32} + 1$ — нет. Докажите это, пользуясь тем, что $641 = 5^4 + 2^4 = 5 \cdot 2^7 + 1$ делит числа $5^4 \cdot 2^{28} + 2^4 \cdot 2^{28}$ и $5^4 \cdot 2^{28} - 1$.

26*. Докажите, что $(f_n, f_m) = 1$ при $n \neq m$. Выведите отсюда, что простых чисел бесконечно много.

27*. Докажите, что в последовательности $2^n - 3$

- а) бесконечно много чисел, делящихся на 5;
- б) бесконечно много чисел, делящихся на 13;
- в) нет чисел, делящихся на $5 \cdot 13$;
- г) бесконечно много попарно взаимно простых чисел.

28. Докажите, что не все натуральные числа представимы в виде суммы а) трех квадратов; б) трех кубов целых чисел.

У к а з а н и е. Использовать признаки делимости на 8 и на 9.

29. (Эратосфен ***) Докажите, что для составного n наименьший простой делитель не превосходит $\sqrt{n}$.

§ 1.3. Алгоритм Евклида и цепные дроби

Свой знаменитый алгоритм **** Евклид придумал для решения задачи о *соизмеримости* двух отрезков.

* М. Мерсенн (Marin Mersenne, 1588–1648) — монах из ордена миноритов, которому писали письма о своих открытиях Ферма, Декарт и Паскаль. В условиях отсутствия научных журналов через него они узнавали о достижениях своих коллег.

** П. Ферма (Pierre de Fermat, 1601–1665) — великий французский математик. Был советником парламента в Тулузе.

*** Эратосфен Киренский (Ερατοσθένης, 276–194 до н. э.) — выдающийся древнегреческий математик и географ.

**** Сам он свой метод алгоритмом, конечно, не называл, термин этот стал популярен позднее и происходит от искажения имени Аль Хорезми (Абу Абдалла Мухаммед бен Муса аль Маджуси, 787–850), жившего в Хорезме выдающегося математика, название одной из книг которого (Китаб мухтасар аль-джебр ва-л-мукабала) дало имя алгебре.

Общей мерой отрезков с длинами l_1 и l_2 называется такой отрезок длины l , который можно уложить без остатка как в первом отрезке (очевидно, ровно l_1/l раз), так и во втором (соответственно l_2/l раз).

В геометрических терминах алгоритм можно описать следующим образом. Меньший отрезок l_2 укладывается в большем l_1 максимально возможное число, скажем a_1 , раз, после чего остается отрезок длины $l_1 - a_1 l_2$, которую обозначим l_3 (на алгебраическом языке это называется *делением с остатком*). Отрезок l_3 укладывается, скажем, a_2 раз в отрезке l_2 и получается в остатке отрезок l_4 . Потом отрезок l_4 укладывается a_3 раз в отрезке l_3 и получается в остатке отрезок l_5 и т. д.

Кстати, сам Евклид индукцию не проводил, а повторил шаг алгоритма три раза, и мы тоже последуем ему в этом. Работу алгоритм заканчивает на том шаге, скажем с номером k , когда полученный на предыдущем шаге отрезок l_{k+1} укладывается на отрезке l_k ровно $a_k = l_k/l_{k+1}$ раз. Тогда в качестве общей меры l отрезков l_1 и l_2 берется отрезок l_{k+1} .

В современной терминологии длину отрезка l_{k+1} — общей меры отрезков l_1 и l_2 — называют *наибольшим общим делителем* l_1 и l_2 и обозначают (l_1, l_2) .

Работу *алгоритма Евклида* можно представить также следующим образом: в прямоугольник размерами $l_1 \times l_2$ укладываем a_1 квадратов размера $l_2 \times l_2$, в оставшийся прямоугольник размерами $l_2 \times l_3$ укладываем a_2 квадратов размера $l_3 \times l_3$ и так далее, пока не покроем прямоугольник размера $l_1 \times l_2$ квадратами k разных размеров в общем количестве $a_1 + \dots + a_k$ штук.

Заметим, что если в процессе применения алгоритма Евклида к числам l_1 и l_2 в результате последовательных делений с остатком получается последовательность частных $a_1, \dots, a_k$, то дробь l_1/l_2 равна так называемой *цепной* (иногда говорят — *непрерывной*) дроби

$$a_1 + \frac{1}{a_2 + \frac{1}{\ddots + \frac{1}{a_{k-1} + \frac{1}{a_k}}}}.$$

Упражнение 2. Докажите это, проверяя последовательно, что

$$\frac{l_{i+1}}{l_i} = a_i + \frac{1}{a_{i+1} + \frac{1}{\ddots + \frac{1}{a_{k-1} + \frac{1}{a_k}}}}, \quad i = k-1, \dots, 1.$$

Поэтому ясно, что произвольную (как правильную, так и неправильную) положительную дробь можно представить в виде цепной дроби с натуральными элементами a_i , а именно

$$a_1 + \frac{1}{a_2 + \frac{1}{\ddots + \frac{1}{a_{k-1} + \frac{1}{a_k}}}},$$

где возможно $a_1 = 0$.



Запись числа в виде цепной дроби неоднозначна, так как

$$\frac{1}{a_k} = \frac{1}{a_k - 1 + \frac{1}{1}}.$$

Чтобы сделать ее однозначной, далее используем только запись, в которой последний элемент $a_k \neq 1$.

Будем использовать также *сокращенную запись цепной дроби*:

$$a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \dots + \frac{1}{a_k}}}.$$

С объявлением однозначности записи числа в виде цепной дроби мы поторопились, так как можно рассматривать цепные дроби с нецелыми элементами. Но для дробей с натуральными элементами это верно: действительно, из равенства

$$\frac{l_1}{l_2} = a_1 + \frac{1}{a_2 + \frac{1}{\ddots + \frac{1}{a_{k-1} + \frac{1}{a_k}}}}$$

следует, что a_1 равно целой части дроби l_1/l_2 , так как дробь

$$\frac{1}{a_2 + \frac{1}{\ddots + \frac{1}{a_{k-1} + \frac{1}{a_k}}}}$$

очевидно меньше 1, и поэтому определяется однозначно. Отсюда следует, что и дробь

$$a_2 + \frac{1}{a_3 + \cfrac{\dots}{\dots + \frac{1}{a_{k-1} + \frac{1}{a_k}}}}$$

определяется однозначно; аналогичным образом получаем, что элемент a_2 определяется однозначно, и т. д.



Алгоритм Евклида заканчивает работу не всегда, а лишь когда отрезки l_1 и l_2 соизмеримы, т. е. когда отношение l_1/l_2 — рациональное число, и только в этом случае соответствующая цепная дробь будет конечной.

Определение 6. Если отрезки несоизмеримы, то число, равное отношению их длин, называется *иррациональным числом*.

В этом случае алгоритм Евклида будет работать бесконечно, и тогда возникнет *бесконечная цепная дробь*.

Упражнение 3. а) Примените алгоритм Евклида для проверки соизмеримости основания и боковой стороны равнобедренного треугольника с углом 72° при основании и проверьте, что алгоритм будет работать бесконечно и породит бесконечную цепную дробь

$$1 + \frac{1}{1 + \cfrac{\dots}{\dots + \frac{1}{1 + \dots}}}$$

б) Найдите геометрически, чему равно отношение боковой стороны к основанию в этом треугольнике, и докажете его иррациональность, не пользуясь алгоритмом Евклида.

Далее иногда удобнее элементы цепной дроби нумеровать, начиная с a_0 . Цепную дробь

$$a_0 + \frac{1}{a_1 + \cfrac{\dots}{\dots + \frac{1}{a_{n-1} + \frac{1}{a_n}}}}$$

можно рассматривать с произвольными, а не только натуральными элементами. Если выполнить все действия, указанные в ней, то ее можно преобразовать в обыкновенную дробь.

Определение 7. Выражение *числителя* и *знаменателя* преобразованной дроби через $a_0, a_1, \dots, a_n$ обозначим $[a_0, \dots, a_n]$ и $[a_1, \dots, a_n]$.

Выражение $[a_0, \dots, a_n]$ представляет из себя многочлен с переменными $a_0, \dots, a_n$.

Упражнение 4. Непосредственно проверьте, что

$$[a_0, \dots, a_n] = a_0[a_1, \dots, a_n] + [a_2, \dots, a_n].$$

Можно считать, что это равенство справедливо и при $n = 1$, если последней скобке в этом случае приписать значение 1.

Применяя алгоритм Евклида к числителю и знаменателю дроби

$$\frac{[a_0, \dots, a_n]}{[a_1, \dots, a_n]},$$

где числа a_i — натуральные, замечаем, что она несократима, так как в результате его работы получается как раз цепная дробь

$$a_0 + \frac{1}{a_1 + \frac{1}{\ddots + \frac{1}{a_{n-1} + \frac{1}{a_n}}}},$$

и

$$([a_0, \dots, a_n], [a_1, \dots, a_n]) = ([a_{n-1}, a_n], [a_n]) = ([a_n], 1) = 1.$$

Со времен Евклида придумано немало новых вариантов его алгоритма, в основном с целью ускорения работы. Опишем некоторые из них.

Обобщенный алгоритм Евклида определяет последовательность вычислений вида

$$\begin{aligned} a &= bq_2 + \varepsilon_2 r_2, & b &= r_2 q_3 + \varepsilon_3 r_3, & r_2 &= r_3 q_4 + \varepsilon_4 r_4, & \dots, \\ r_{k-3} &= r_{k-2} q_{k-1} + \varepsilon_{k-1} r_{k-1}, & r_{k-1} &= r_k q_k, \end{aligned}$$

где

$$\varepsilon_i = \pm 1, \quad 0 < r_i < r_{i-1}, \quad i \geq 1, \quad b = r_1, \quad a = r_0.$$

Число $k - 1$ назовем его длиной. Как и в обычном алгоритме Евклида, $(a, b) = r_k$.

Алгоритмом Евклида с выбором минимального по модулю остатка называется обобщенный алгоритм Евклида, в котором всегда $2r_i \leq r_{i-1}$, т. е. на каждом шаге из двух возможных вариантов деления

$$r_{i-2} = r_{i-1} q_{i-1} + r_i, \quad \text{где } 0 < r_i < r_{i-1},$$

и

$$r_{i-2} = r_{i-1}(q_{i-1} + 1) - (r_{i-1} - r_i)$$

выбираем тот, при котором получается минимальный по абсолютной величине остаток (если они равны по модулю, то берем любой из них).

- Упражнение 5.** а) Если u и v четны, то $(u, v) = 2(u/2, v/2)$;
 б) если u четно, а v нечетно, то $(u, v) = (u/2, v)$;
 в) если u и v нечетны, то $u - v$ четно,

$$|u - v| < \max(u, v), \quad (u, v) = (|u - v|, \min(u, v)).$$

Алгоритм, основанный на этих утверждениях, называется *бинарным вариантом алгоритма Евклида*. Как выяснилось, этот вариант алгоритма Евклида был известен в Древнем Китае (но обычного варианта там не знали).

Задачи и упражнения к § 1.3

1. При каких целых n дробь $\frac{5n+6}{8n+7}$ несократима? Докажите, что дробь $\frac{21n+4}{14n+3}$ несократима при всех целых n .

2. На миллиметровой бумаге нарисован прямоугольник размером $a \times b$ так, что стороны его идут по линиям сетки. На какое число частей делят узлы сетки его диагональ?

3. От нарисованного прямоугольника отрезают несколько квадратов со стороной b до тех пор, пока не останется прямоугольник с шириной меньше b , и с ним поступают точно так же, пока не получится прямоугольник, который целиком разрезается на квадраты. Приведите пример прямоугольника $a \times b$, который разрезается ровно на n квадратов.

4. Пусть $(m, 360) = 1$, $1 < m < 360$. Докажите, что с помощью одного циркуля можно разделить угол в m градусов на m равных частей.

5. Примените бинарный алгоритм для доказательства равенства

$$(2^m - 1, 2^n - 1) = 2^{(m,n)} - 1.$$

6. Докажите, что при любом целом $a \neq 1$ имеем $(a^m - 1, a^n - 1) = a^{(m,n)} - 1$.

7. Докажите иррациональность квадратного корня из любого натурального числа, не являющегося полным квадратом (т. е. квадратом натурального числа).

8. Примените алгоритм Евклида для доказательства открытой, по преданию, Пифагором несоизмеримости диагонали квадрата с его стороной.

9. Разложите $\sqrt{2}$ в цепную дробь.

10. (Эйлер *.) Докажите индукцией по n , что выражение (называемое иногда *континуантом*, или *скобками Эйлера*)

$$[a_0, \dots, a_n]$$

можно получить следующим образом: берем произведение всех элементов, затем всевозможные произведения, которые можно получить, опустив какую-нибудь пару соседних элементов, затем из этих произведений получаем новые, выбрасывая произвольным образом пары соседних элементов, и так далее, и, наконец, суммируем все различные из получившихся произведений (если $n + 1$ четно, то на последнем шаге получается «пустое» произведение, не содержащее вообще сомножителей; как принято, его значение по определению полагаем равным 1).

11. Докажите, что $[a_0, \dots, a_n] = [a_n, \dots, a_0]$, т. е. при изменении порядка элементов на противоположный числитель дроби не меняется.

12. Докажите, что $[a_0, \dots, a_n] = a_n[a_0, \dots, a_{n-1}] + [a_0, \dots, a_{n-2}]$.

Определение 8. Дробь, образованная первыми k этажами, называется k -й *подходящей дробью* для исходной дроби. Ее величина изображается обыкновенной дробью $\frac{[a_0, \dots, a_k]}{[a_1, \dots, a_k]}$, которую для краткости далее обозначаем p_k/q_k .

Определение 9. Дробь $\frac{[a_{k+1}, \dots, a_n]}{[a_{k+2}, \dots, a_n]}$ называется k -м *остатком* и обозначается r_k .

13. Проверить, что $\frac{[a_0, \dots, a_n]}{[a_1, \dots, a_n]} = \frac{[a_0, \dots, a_k, r_k]}{[a_1, \dots, a_k, r_k]}$.

14. Докажите, что при $k \geq 2$ справедливы равенства

$$p_k = a_k p_{k-1} + p_{k-2}, \quad q_k = a_k q_{k-1} + q_{k-2}.$$

15*. (Конструкция для наименьших решений в натуральных числах уравнения $ax - by = 1$.) Разложим $\frac{a}{b}$ в цепную дробь

$$\frac{a}{b} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \ddots + \frac{1}{a_{n-1} + \frac{1}{a_n}}}}.$$

* Л. Эйлер (Leonhard Euler, 1707–1783) — один из самых знаменитых математиков в истории. Родился в Базеле (Швейцария), большую часть своей жизни провел в Санкт-Петербурге, будучи членом Петербургской академии наук.

Заменяя в случае необходимости a_n на $(a_n - 1) + \frac{1}{1}$, можно считать, что n нечетно. Докажите, что наименьшее решение в натуральных числах уравнения $ax - by = 1$ есть $x = q_{n-1}$, $y = p_{n-1}$.

Обозначим $L(a, b)$ минимальную длину обобщенного алгоритма Евклида для вычисления (a, b) , а $L_0(a, b)$ — длину алгоритма Евклида с выбором минимального по модулю остатка.

16*. (Кронекер *.) Докажите, что $L_0(a, b) \leq L(a, b)$.

17*. (Дюпре **.) Докажите, что

$$L_0(a, b) \leq \min \{ \lfloor \log_\alpha (2\sqrt{2} \min(a, b) + \sqrt{2}) \rfloor, \lfloor \log_\alpha (2\sqrt{2}(a+b) + \sqrt{2}) \rfloor - 1 \},$$

где $\alpha = \sqrt{2} + 1$.

18*. Алгоритм Евклида с выбором минимального по модулю остатка на каждом шаге не более чем вдвое короче по числу шагов деления обычного алгоритма Евклида. Оценка достигается на паре (F_{2n-1}, F_{2n}) .

19.** (Д. Кнут.) Число вычитаний, выполняемых бинарным алгоритмом в применении к паре чисел u, v , не больше $1 + \lfloor \log_2 \max(u, v) \rfloor$ и равенство возможно, лишь когда $\lfloor \log_2(u+v) \rfloor > \lfloor \log_2 \max(u, v) \rfloor$.

§ 1.4. Числа Фибоначчи

Определение 10. Последовательность $\{F_n\}$, определенная равенствами

$$F_0 = 0, \quad F_1 = 1, \quad F_n = F_{n-1} + F_{n-2}, \quad n = 2, 3, 4, \dots,$$

называется *последовательностью Фибоначчи* ***.

Числа Фибоначчи тесно связаны с цепными дробями и алгоритмом Евклида.

Например, обозначив n -этажную цепную дробь $1 + \frac{1}{1+} \dots \frac{1}{+1}$ через φ_n и преобразовывая ее от n -этажного вида к обыкновенному, получим дробь $F_{n+1}/F_n = \varphi_n$.

Связь с цепными дробями видна также в следующей лемме.

Лемма 2. Число одночленов в многочлене $[a_1, \dots, a_n]$ равно F_{n+1} и при любых натуральных $a_1, \dots, a_n$ справедливо неравенство $F_{n+1} \leq [a_1, \dots, a_n]$, которое обращается в равенство, лишь когда $a_1 = \dots = a_n = 1$.

* Л. Кронекер (Leopold Kronecker, 1823–1891) — известный немецкий математик. Автор афоризма: «Господь создал натуральные числа. Остальное дело рук человека».

** Французский математик Дюпре доказал эту теорему в середине XIX в.

*** Она появилась в XIII столетии в книге Леонардо Пизанского, по прозвищу Фибоначчи (Leonardo da Pisa, Fibonacci, ок. 1170–1228), в задаче, в которой шла речь о размножении кроликов.

Д о к а з а т е л ь с т в о. Первое утверждение леммы следует из второго, поэтому достаточно доказать индукцией по n , что $F_{n+1} \leq [a_1, \dots, a_n]$, причем равенство $F_{n+1} = [a_1, \dots, a_n]$ справедливо, лишь когда $a_1 = \dots = a_n = 1$.

Удобно начинать индукцию с $n = 0$, полагая формально, как и раньше, $[a_1, \dots, a_n] = 1$, $F_{1+a_1+\dots+a_n} = F_1 = 1$ при $n = 0$, тогда неравенства леммы очевидно обращаются в равенства.

База индукции ($n = 0, 1$) теперь очевидна. Проведем индукционный переход. Согласно равенству

$$[a_1, \dots, a_n] = a_1[a_2, \dots, a_n] + [a_3, \dots, a_n]$$

и предположению индукции, справедливы неравенства

$$F_n \leq [a_2, \dots, a_n], \quad F_{n-1} \leq [a_3, \dots, a_n],$$

следовательно,

$$F_{n+1} = F_n + F_{n-1} \leq [a_2, \dots, a_n] + [a_3, \dots, a_n] \leq [a_1, \dots, a_n]$$

и равенство $F_{n+1} = [a_1, \dots, a_n]$ справедливо лишь при $a_1 = \dots = a_n = 1$. $\square$

Обозначая предел последовательности φ_n через φ и переходя к пределу в обеих частях равенства

$$\varphi_n = 1 + \frac{1}{\varphi_{n-1}},$$

получаем уравнение

$$\varphi = 1 + \frac{1}{\varphi},$$

у которого на роль φ годится только положительный корень

$$\varphi = (\sqrt{5} + 1)/2$$

— так называемое *золотое сечение*.

Среди огромного числа фактов о числах Фибоначчи мы приведем только небольшое количество.

Лемма 3. Для чисел Фибоначчи справедливо тождество

$$F_{n+m} = F_m F_{n+1} + F_{m-1} F_n, \quad m \geq 1, \quad n \geq 0.$$

Д о к а з а т е л ь с т в о. Доказательство тождества проведем индукцией по m . База индукции при $m = 1, 2$ очевидно справедлива, а для выполнения шага индукции достаточно проверить равенство

$$\begin{aligned} F_{n+m+1} &= F_{n+m} + F_{n+m-1} = (F_m F_{n+1} + F_{m-1} F_n) + (F_{m-1} F_{n+1} + F_{m-2} F_n) = \\ &= (F_m + F_{m-1}) F_{n+1} + (F_{m-1} + F_{m-2}) F_n = F_{m+1} F_{n+1} + F_m F_n. \end{aligned} \quad \square$$

Следующая теорема довольно удивительна: в ней целое число выражается через иррациональное.

Теорема 6 (Бине *). *Справедлива формула*

$$F_n = \frac{\varphi^n - (-\varphi)^{-n}}{\sqrt{5}}.$$

Доказательство. Доказательство также проведем по индукции. База индукции при $n = 0, 1$ очевидно справедлива, так как

$$\frac{\varphi - (-\varphi)^{-1}}{\sqrt{5}} = \frac{\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}}{\sqrt{5}} = 1,$$

а для выполнения шага индукции достаточно проверить равенства

$$\varphi^2 = \varphi + 1, \quad (-\varphi)^{-2} = (-\varphi)^{-1} + 1,$$

из них выведите почленным умножением равенства

$$\varphi^{n+1} = \varphi^n + \varphi^{n-1}, \quad (-\varphi)^{-n-1} = (-\varphi)^{-n} + (-\varphi)^{-n+1}$$

и заметить, что тогда

$$\begin{aligned} F_{n+1} &= F_n + F_{n-1} = \\ &= \frac{\varphi^n - (-\varphi)^{-n}}{\sqrt{5}} + \frac{\varphi^{n-1} - (-\varphi)^{-n+1}}{\sqrt{5}} = \frac{\varphi^{n+1} - (-\varphi)^{-n-1}}{\sqrt{5}}. \quad \square \end{aligned}$$

Напомним, что целой частью числа x называется наибольшее целое число n такое, что $n \leq x$. Обозначается целая часть символом $\lfloor x \rfloor$.

Лемма 4. *Неравенство $F_n \leq t$ справедливо тогда и только тогда, когда*

$$n \leq \lfloor \log_{\varphi} (\sqrt{5}(t + 1/2)) \rfloor.$$

Неравенство $F_n \geq t$ справедливо тогда и только тогда, когда

$$n \geq \lfloor \log_{\varphi} (\sqrt{5}(t - 1/2)) \rfloor + 1.$$

Доказательство. Для доказательства леммы перепишем неравенство $F_n \leq t$ с помощью формулы Бине в виде

$$\frac{\varphi^n - (-\varphi)^{-n}}{\sqrt{5}} \leq t,$$

что равносильно неравенствам

$$\frac{\varphi^n}{\sqrt{5}} \leq t + \frac{(-\varphi)^{-n}}{\sqrt{5}} < t + \frac{1}{2},$$

* Ж. Бине (Jacques Philippe Marie Binet, 1786–1856) — французский математик и астроном, член Парижской академии наук.

так как если

$$\frac{\varphi^n}{\sqrt{5}} < m + \frac{1}{2},$$

то

$$F_n = \frac{\varphi^n - (-\varphi)^{-n}}{\sqrt{5}} < m + \frac{1}{2} - \frac{(-\varphi)^{-n}}{\sqrt{5}} < m + 1,$$

и значит, $F_n \leq m$. Неравенство

$$\frac{\varphi^n}{\sqrt{5}} < m + \frac{1}{2}$$

равносильно

$$n < \log_{\varphi} (\sqrt{5}(m + 1/2)),$$

а значит, и неравенству

$$n \leq \lfloor \log_{\varphi} (\sqrt{5}(m + 1/2)) \rfloor,$$

так как $\log_{\varphi} (\sqrt{5}(m + 1/2))$ не может быть целым числом, ведь в противном случае

$$\frac{\varphi^k}{\sqrt{5}} = m + 1/2,$$

откуда

$$F_k = \frac{\varphi^k - (-\varphi)^{-k}}{\sqrt{5}} = m + \frac{1}{2} - \frac{(-\varphi)^{-k}}{\sqrt{5}} = m + \alpha, \quad 0 < \alpha < 1,$$

что невозможно, так как F_k — целое число.

Второе утверждение леммы очевидно равносильно первому. $\square$

Отметим, что из леммы вытекает, что последовательность

$$\Phi(m) = \lfloor \log_{\varphi} (\sqrt{5}(m + 1/2)) \rfloor$$

обратна к последовательности Фибоначчи F_n в том смысле, что

$$\Phi(F_n) = n.$$

Теорема 7 (Дюпре). *Наибольшее число делений в алгоритме Евклида нахождения (a, b) не превосходит*

$$\lfloor \log_{\varphi} (\sqrt{5} (\min(a, b) + 1/2)) \rfloor.$$

Оценка точная.

Доказательство. Можно считать, что $a > b$. Пусть число делений равно $k + 1$, значит, a/b представимо k -этажной дробью

$$\frac{[a_0, \dots, a_k]}{[a_1, \dots, a_k]},$$

а так как $[a_0, \dots, a_k]$ и $[a_1, \dots, a_k]$ взаимно просты, то

$$[a_1, \dots, a_k] \leq b,$$

и из леммы 2 следует, что $F_k \leq b$, а из леммы 4 следует, что

$$k \leq \lfloor \log_{\varphi} (\sqrt{5}(b + 1/2)) \rfloor. \quad \square$$

На практике более удобно для применения следующее утверждение.

Следствие из теоремы 7 (Ламе *). *Наибольшее число делений в алгоритме Евклида нахождения (a, b) не превосходит $5k$, где k — число десятичных знаков в наименьшем из чисел a, b .*

Задачи и упражнения к § 1.4

1. Проверьте, что F_n — ближайшее целое к числу $\varphi^n/\sqrt{5}$.
2. Докажите следствие из теоремы 7.
3. Сколькими способами можно замостить прямоугольник размера $2 \times n$ фишками домино размера 1×2 ?

У к а з а н и е. Можно применить задачу 10 из § 1.3 и лемму 3.

4. Сколько подмножеств можно выбрать в множестве чисел от 1 до n , не включающих двух соседних чисел?

У к а з а н и е. Можно применить задачу 10 из § 1.3 и лемму 3.

5. Докажите, что $F_{m+1}F_n - F_mF_{n+1} = (-1)^m F_{n-m}$.

6. Докажите, что $(F_n, F_{n+1}) = 1$.

7. Если продолжить последовательность Фибоначчи в «отрицательную» сторону с сохранением равенства $F_n + F_{n+1} = F_{n+2}$, то будут выполняться равенства $F_{-k-1} = (-1)^k F_k$ и сохранятся все формулы предыдущих задач.

Следующая задача обобщает задачу 6.

- 8*. (Люка **.) Докажите, что $(F_n, F_m) = F_{(n,m)}$.

9. Последовательность Фибоначчи содержит бесконечно много попарно взаимно простых чисел.

- 10*. Вместо чисел Фибоначчи рассмотрим остатки от их деления на данное число m . Докажите, что последовательность остатков является чисто периодической с периодом, не большим $m^2 - 1$.

11. В случае $m = F_k$ найдите точно период последовательности из предыдущей задачи.

- 12*. Найдите остаток от деления F_n на F_k .

* Г. Ламе (Gabriel Lamé, 1795–1870) — французский инженер и математик, член Парижской и Петербургской академий наук.

** Эдуард Люка (Eduard Lucas, 1842–1891) — известный французский специалист по теории чисел и педагог, автор множества красивых задач и четырехтомника о математических развлечениях, сильно сокращенный перевод которого был издан в 1885 г. в Санкт-Петербурге и с тех пор, к сожалению, не перензадавался.

13*. Докажите, что разложение числа F_{n-3}/F_n в цепную дробь имеет вид

$$\cfrac{1}{4 + \cfrac{\ddots}{\ddots + \cfrac{1}{4 + a_k}}},$$

где $k = 1 + m$, $a_k = 0$ при $n = 3m$, $a_k = 1/3$ при $n = 3m + 1$, $a_k = 1/5$ при $n = 3m + 2$.

14*. Подмножество множества чисел от 1 до n назовем эгоистичным, если оно содержит число, равное своей мощности. Чему равно число эгоистичных подмножеств?

§ 1.5. Квадратные уравнения

Первое нетривиальное алгебраическое уравнение — квадратное, т. е. уравнение вида $x^2 + px + q = 0$, — было решено в глубокой древности. Это уравнение легко свести к уравнению вида $x^2 = c$, которое для неотрицательных c решается с помощью арифметического квадратного корня:

$$x_1 = \sqrt{c}, \quad x_2 = -\sqrt{c}$$

— два его решения. Для этого достаточно выделить полный квадрат:

$$x^2 + px + q = x^2 + 2\frac{p}{2}x + \left(\frac{p}{2}\right)^2 - \left(\frac{p}{2}\right)^2 + q = \left(x + \frac{p}{2}\right)^2 + q - \left(\frac{p}{2}\right)^2.$$

Получаем формулу для корней исходного уравнения:

$$x_1 = -\frac{p}{2} + \sqrt{\left(\frac{p}{2}\right)^2 - q}, \quad x_2 = -\frac{p}{2} - \sqrt{\left(\frac{p}{2}\right)^2 - q}$$

в случае, если $\left(\frac{p}{2}\right)^2 - q \geq 0$.

Заметим, что квадрат разности корней легко выражается через коэффициенты

$$(x_1 - x_2)^2 = p^2 - 4q = D.$$

Это выражение называется *дискриминантом* уравнения; оно содержит значительную информацию о корнях. В самом деле, по определению $D = 0$ тогда и только тогда, когда корни уравнения совпадают (в этом случае говорят, что уравнение имеет *кратный* корень). Если $D \geq 0$, то у уравнения есть действительные корни. В противном случае их нет.

Для квадратного уравнения $x^2 + px + q = 0$ справедлива *теорема Виета*: сумма корней уравнения равна $-p$, а произведение равно q .

Далее она будет сформулирована в общем виде, а сейчас предлагается в качестве упражнения.

Упражнение 6. Выведите эту теорему из формулы для корней квадратного уравнения.

Квадратные уравнения изучают уже в восьмом классе, поэтому мы написали о них бегло. Однако огромное количество ошибок, допускаемых школьниками и абитуриентами, появляется именно в решении квадратных уравнений. Основная причина, конечно, невнимательность. Часто, например, при решении их «в уме» путаются две разные формулы для корней уравнения, которые даются в школьном учебнике, и из них составляется одна неверная.

Речь идет, конечно, о формуле для решения квадратного уравнения в виде $ax^2 + bx + c = 0$.

Упражнение 7. Выведите эту формулу из старой формулы.

Иногда забывают, что и теорема Виета для уравнения в виде $ax^2 + bx + c = 0$ выглядит чуть по-другому.

Упражнение 8. Запишите теорему Виета для уравнения $ax^2 + bx + c = 0$.

Дадим несколько советов, как избегать таких ошибок. Первый из них: не переоценивайте свои способности к устному счету, лучше напишите формулу на бумаге, проверьте, что это та формула, которая нужна, подставьте в нее численные значения коэффициентов, не перепутав их друг с другом. Если коэффициенты большие, то увеличивается вероятность арифметической ошибки при вычислении дискриминанта. Так как из него потом надо извлекать корень, иногда полезно сразу его разлагать на множители, если коэффициенты имеют общие делители, или применять формулу разности квадратов и найденные множители выносить за знак корня, извлекая из них при этом корень.

Например, если при решении уравнения $45x^2 + 42x + 5 = 0$ получились формула для корней

$$x_{1,2} = \frac{-42 \pm \sqrt{42^2 - 4 \cdot 45 \cdot 5}}{2 \cdot 45},$$

то так как

$$42^2 - 4 \cdot 45 \cdot 5 = 4 \cdot 9 \cdot (7^2 - 5^2) = 4 \cdot 9 \cdot 2 \cdot 12 = 4 \cdot 9 \cdot 4 \cdot 6 = (4 \cdot 3)^2 \cdot 6 = 12^2 \cdot 6,$$

ответом будет

$$x_{1,2} = \frac{-42 \pm 12\sqrt{6}}{2 \cdot 45} = \frac{-7 \pm 2\sqrt{6}}{15}.$$

В тех случаях, когда уравнение имеет целые корни, их проще угадать с помощью теоремы Виета, чем находить по формуле.

Упражнение 9. Угадайте корни квадратного уравнения $\frac{1}{12}x^2 + \frac{7}{12}x = 19$ из книги Аль Хорезми.

При применении этого приема к уравнению $x^2 + 2001x + 2000 = 0$ могут возникнуть затруднения из-за большого числа возможных вариантов. Но легко заметить и без теоремы Виета, что один из корней равен -1 . Второй корень находится уже с помощью этой теоремы: $x_2 = -2000$. Забудьте, что использование формулы приводит к довольно громоздким вычислениям.

Но бездумное использование теоремы Виета может привести к ошибке, например, в следующей задаче.

Упражнение 10. Числа p и q — корни уравнения $x^2 + px + q = 0$. Чему могут быть равны эти числа?

Действительно, применяя теорему Виета, получаем систему уравнений

$$\begin{cases} p + q = -p; \\ pq = q, \end{cases}$$

откуда имеем $p = 1$, $q = -2p = -2$; $q = p = 0$.

Но это не все решения! Дело в том, что если $p = q \neq 0$, из условия ясно только, что p — корень уравнения, а про второй корень ничего не сказано. Поэтому проще теорему Виета не применять, а подставить $x = p$, q в уравнение и получить систему

$$\begin{cases} 2p^2 + q = 0; \\ q^2 + pq + q = 0, \end{cases}$$

откуда $q_1 = p_1 = 0$ и при $q \neq 0$ имеем $q = -p - 1$, $2p^2 - p - 1 = 0$, значит, $p_{2,3} = 1, -1/2$, $q_{2,3} = -2, -1/2$.

Чтобы читатель не подумал, что он уже знает о квадратных уравнениях все, приведем несколько примеров любопытных задач, связанных с ними.

Упражнение 11. Проверьте справедливость следующей, правда, совершенно бесполезной с практической точки зрения, формулы для корней квадратного уравнения $x^2 + px + q = 0$, именно

$$x_{1,2} = \frac{p \pm c\sqrt{p^2 - 4q} + 2q}{2c + p \mp \sqrt{p^2 - 4q}}.$$

В ней c — произвольный параметр, удовлетворяющий лишь условию

$$2c + p \mp \sqrt{p^2 - 4q} \neq 0,$$

т. е. это фактически бесконечное семейство разных формул для решения уравнения $x^2 + px + q = 0$. Обычная формула является предельным случаем указанной формулы.

Следующая задача является частным случаем одной из теорем Чебышёва.

Упражнение 12. Среди всех квадратных трехчленов $x^2 + px + q = 0$ найдите тот, у которого максимальное по модулю значение на отрезке $[-1, 1]$ минимально (т. е. тот, который *наименее отклоняется от нуля* на этом отрезке).

В таких задачах труднее всего найти ответ, но если он найден, то доказать его правильность уже проще. Поэтому ответ мы сразу подскажем: искомый экстремальный трехчлен есть $x^2 - 1/2$, а его уклонение от нуля, т. е. максимум на отрезке $[-1, 1]$, равно $1/2$.

Если же взять любой трехчлен $f(x) = x^2 + px + q$, то, заметив, что

$$f(-1) - 2f(0) + f(1) = 2$$

независимо от p, q , выводим отсюда неравенство

$$4m \geq |f(-1)| + 2|f(0)| + |f(1)| \geq |f(-1) - 2f(0) + f(1)| = 2,$$

где m — упомянутый максимум.

Но этого недостаточно, нужно доказать строгое неравенство при $f(x) \neq x^2 - \frac{1}{2}$. Для этого найдем условие, когда доказанное неравенство превращается в равенство. Необходимое условие есть

$$f(-1) = f(1) = -f(0) = 1/2.$$

Ясно, что этому условию удовлетворяет только трехчлен $x^2 - 1/2$, так как система уравнений

$$\begin{cases} 1 + q - p = 1/2; \\ 1 + q + p = 1/2; \\ q = -1/2 \end{cases}$$

имеет единственное решение $p = 0, q = -1/2$.

Упражнение 13. Пусть x_i — корни уравнения $x^2 + px + q = 0$. Вычислите $x_1^{10} + x_2^{10}$.

Попытка решить эту задачу с помощью формул для корней квадратного уравнения приводит к громоздким вычислениям. Укажем подход, который позволяет решать любые задачи подобного вида, не используя формул для корней квадратного уравнения.

Для этого заметим, что последовательность $a_n = x_1^n + x_2^n$, так же как и произвольная последовательность вида $a_n = bx_1^n + cx_2^n$, удовлетворяет

следующему соотношению (такие соотношения называют *рекуррентными*)

$$a_{n+2} + pa_{n+1} + qa_n = 0.$$

Действительно,

$$\begin{aligned} a_{n+2} + pa_{n+1} + qa_n &= x_1^{n+2} + x_2^{n+2} + p(x_1^{n+1} + x_2^{n+1}) + q(x_1^n + x_2^n) = \\ &= x_1^n(x_1^2 + px_1 + q) + x_2^n(x_2^2 + px_2 + q) = 0. \end{aligned}$$

С помощью этого соотношения можно последовательно вычислять по формуле $a_{n+2} = -pa_{n+1} - qa_n$, нужно только знать первые два значения a_0 и a_1 . Но $a_0 = x_1^0 + x_2^0 = 2$, а $a_1 = x_1^1 + x_2^1 = -p$ по теореме Виета. Если вам не нравится формула $a_0 = x_1^0 + x_2^0$, можно вместо нее взять $a_2 = x_1^2 + x_2^2$, результат будет тот же, но придется выразить $a_2 = x_1^2 + x_2^2 = (x_1 + x_2)^2 - 2x_1x - 2 = p^2 - 2q$.

Теперь уже легко найти a_{10} и вообще любое значение a_n , причем ясно, что это значение будет всегда целым числом, если p, q сами целые.

Но еще больший интерес представляет обратная задача. Пусть дана последовательность a_n , удовлетворяющая *линейному рекуррентному соотношению второго порядка*

$$a_{n+2} + pa_{n+1} + qa_n = 0$$

и начальным условиям $a_0 = a, a_1 = b$. Надо найти явную формулу для этой последовательности. Частный случай (последовательность Фибоначчи) уже рассматривался нами ранее.

В общем случае действуем следующим образом. Заметим, что как уже было проверено выше, любая последовательность вида $a_n = cx_1^n + dx_2^n$, где x_i — корни уравнения $x^2 + px + q = 0$, а c и d — константы, удовлетворяет соотношению $a_{n+2} = -pa_{n+1} - qa_n$. Если корни x_i различны, то для любых начальных условий $a_0 = a, a_1 = b$ можно однозначно найти коэффициенты c, d , решив систему уравнений

$$\begin{cases} c + d = a; \\ cx_1 + dx_2 = b. \end{cases}$$

Тогда последовательность $a_n = cx_1^n + dx_2^n$ совпадает с заданной, так как удовлетворяет тому же соотношению и тем же начальным условиям.

Упражнение 14. Проверьте, что в случае $x_1 = x_2$ последовательность a_n можно искать в виде $cx_1^n + dnx_1^n$, где c и d — константы.

Задачи и упражнения к § 1.5

1. Решите уравнение Иоганна Мюллера *

$$\frac{x}{10-x} + \frac{10-x}{x} = 25.$$

2. Решите уравнение $x^2 + 1999x + 1998 = 0$.
 3. Решите уравнение $1999x^2 + 1000x - 2999 = 0$.
 4. Если уравнение $a + bx + cx^2 = 0$ имеет только действительные корни, то это же верно для уравнения $a + bx + cx^2/2 = 0$.
 5. Пусть x_1, x_2 — корни уравнения $1 + kx + x^2 = 0$. Найдите все k , при которых справедливо неравенство $(x_1/x_2) + (x_2/x_1) > 1$.
 6. Найдите все a , для которых корни уравнения $4x^2 - 2x + a = 0$ заключены между -1 и 1 .
 7. Для каких a уравнение $(3a + 2)x^2 + (a - 1)x + 4a + 3 = 0$ имеет один корень больше 3, а другой — меньше 2?
 8. Если a, b, c — стороны треугольника, то уравнение

$$b^2x^2 + (b^2 + c^2 - a^2)x + c^2 = 0$$

не имеет действительных корней.

9. Сколько существует уравнений вида $x^2 - px - q = 0$, где p и q — натуральные числа, положительный корень которых меньше заданного натурального числа r ?

- 10*. Докажите, что если

$$(q_2 - q_1)^2 + p_1^2q_2 + p_2^2q_1 - p_1p_2(q_2 + q_1) < 0,$$

то корень одного из уравнений $x^2 + p_ix + q_i = 0$ лежит между корнями другого.

11. Если все корни уравнений $x^2 + p_ix + q_i = 0$ по модулю меньше 1, то все корни уравнения $x^2 + (p_1 + p_2)x/2 + (q_1 + q_2)/2 = 0$ по модулю меньше 1.

12. Если x_i — корни уравнения $x^2 - 6x + 1 = 0$, то $x_1^n + x_2^n$ — целое число при натуральном n , не кратное 5.

13. Пусть x_i — корни уравнения $x^2 + px + q = 0$. Найдите квадратное уравнение с корнями x_1^n, x_2^n .

14. Пусть x_i — корни уравнения $x^2 + px + 1 = 0$, p — нечетное. Докажите, что $x_1^n + x_2^n$ — целое число при любом натуральном n и $(x_1^{n+1} + x_2^{n+1}) = 1$.

* И. Мюллер (Johannes Müller, Regiomontanus, 1436–1476), по прозвищу Региомонтан — немецкий математик.

15. Пусть x_i — корни уравнения $ax^2 + bx + c = 0$. Найдите $x_1^{-3} + x_2^{-3}$.

16. Найдите формулу для последовательности

$$a_{n+1} = 3a_n - 2a_{n-1}, \quad a_1 = 1, \quad a_0 = 0.$$

17. Найдите формулу для последовательности

$$a_{n+1} = 4a_n - 4a_{n-1}, \quad a_1 = 1, \quad a_0 = 0.$$

18*. Квадратный трехчлен $ax^2 + bx + c$ на отрезке $[0, 1]$ принимает значения, не большие по модулю 1. Какое максимальное значение может иметь при этом сумма $|a| + |b| + |c|$?

19. Квадратный трехчлен при любом целом x принимает значения, равные четвертой степени натурального числа. Докажите, что он равен константе.

20*. Квадратный трехчлен при любом целом x принимает значения, равные квадрату натурального числа. Докажите, что он равен квадрату многочлена первой степени.

§ 1.6. Комбинаторика отображений

Далее с целью краткости будем использовать следующие общепринятые обозначения* (которыми постараемся не злоупотреблять).

Конечные множества будем задавать, перечисляя их элементы в фигурных скобках, например, $\{1, 3, 5\}$.

Произвольное множество A будем иногда задавать в виде $\{x: A(x)\}$, где $A(x)$ — некоторое утверждение, которое является истинным тогда и только тогда, когда x принадлежит множеству A , например, конечное множество натуральных чисел $\{n, n+1, \dots, m\}$ можно определить и так: $\{x: n \leq x \leq m\}$. Используем также обозначения:

$e \in E$ — e является элементом множества E ;

$A \subset E$ — множество A является подмножеством множества E ;

$A \cup B$ — объединение множеств A и B ;

$A \cap B$ — пересечение множеств A и B ;

$A \setminus B$ — разность множеств A и B , т.е. множество всех элементов из A , не принадлежащих множеству B .

В качестве упражнения пусть читатель проверит, что

$$A \setminus B = A \setminus (A \cap B), \quad A \setminus (A \setminus B) = A \cap B, \quad A \cup B = A \cup (B \setminus A).$$

Запись $P \Rightarrow Q$ будет означать, что из утверждения P следует утверждение Q (читается: «если P , то Q »). Сразу предупредим читателя,

* Теоретико-множественные обозначения и терминология, используемая далее, стали общепринятыми после работ Г. Кантора.

что если утверждение P ложно, то утверждение $P \Rightarrow Q$ в математике (но не всегда в философии) считается истинным независимо от истинности или ложности утверждения Q . (Действительно, из ложного утверждения можно логически безупречно вывести как истинные, так и ложные утверждения.)

Запись $P \Leftrightarrow Q$ будет означать, что утверждение P равносильно утверждению Q . Заметим, что $P \Leftrightarrow Q$ имеет место тогда и только тогда, когда $P \Rightarrow Q$ и $Q \Rightarrow P$. Многие теоремы имеют вид равносильности двух утверждений (например, « P справедливо тогда и только тогда, когда справедливо Q »). Для их доказательства мы и будем пользоваться этим простым замечанием (а именно, предполагая верным P , выводять из него Q , а потом, предполагая верным Q , выводять из него P). Например, для доказательства равенства множеств A и B будем вначале доказывать, что $A \subset B$ (A содержится в B), а потом — что $B \subset A$ (B содержится в A).

Остальные обозначения будут вводиться по ходу изложения.

Пусть $A_1, \dots, A_n$ — конечные непустые множества.

Определение 11. Упорядоченный набор $(a_1, \dots, a_n)$, компоненты которого a_i принадлежат множествам A_i , $i = 1, \dots, n$, назовем *словом*. Множество всех таких слов обозначим $A_1 \times \dots \times A_n$ и назовем *декартовым* произведением* множеств $A_1, \dots, A_n$.

Примеры. 1. Если $A_1 = \{a, b, c, d, e, f, g, h\}$, $A_2 = \{1, 2, 3, 4, 5, 6, 7, 8\}$, то $A_1 \times A_2$ — шахматная доска (рис. 1).

2. Если A — алфавит русского языка, то среди префиксов (т. е. начал) всевозможных слов множества $\underbrace{A \times \dots \times A}_{30}$ встречаются все слова русского языка.

Далее вместо $\underbrace{A \times \dots \times A}_{n \text{ раз}}$ используем краткое обозначение A^n , называемое *декартовой степенью* множества A .

Примеры. 1. Если множество $A = E_2 = \{0, 1\}$, то его декартова степень $A^n = E_2^n$ состоит из всех слов длины n , составленных из 0 и 1. Это множество называют *n -мерным двоичным кубом*.

2. Если множество $A = E_k = \{0, 1, \dots, k-1\}$, то его декартова степень $A^n = E_k^n$ состоит из всех слов длины n , составленных из $0, 1, \dots, k-1$. Это множество называют *n -мерным k -ичным кубом*.

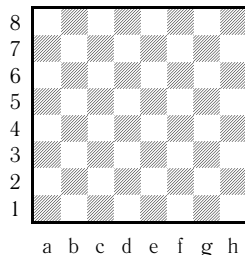


Рис. 1

* Р. Декарт (René Descartes, 1596–1650) — великий французский философ и математик.

3. Если множество $A = \mathbb{R}$ — множество всех действительных чисел, то его декартова степень $A^n = \mathbb{R}^n$ состоит из всех n -мерных векторов с действительными координатами и называется *n -мерным арифметическим пространством*.

4. При $n = 2$ в предыдущем примере получается плоскость, а при $n = 3$ — трехмерное арифметическое пространство. Именно этот пример по существу имел в виду Декарт, когда вводил в геометрию координаты.

Число элементов конечного множества A называют его *мощностью* и обозначают $|A|$.

Теорема 8 (принцип умножения). *Справедливо равенство*

$$|A_1 \times \dots \times A_n| = |A_1| \cdot \dots \cdot |A_n|$$

(словесная формулировка: число элементов в декартовом произведении множеств равно произведению мощностей этих множеств).

Доказательство. Индукция по n . База: $n = 2$. Если $A_2 = \{a_{21}, \dots, a_{2n_2}\}$, то

$$A_1 \times A_2 = (A_1 \times \{a_{21}\}) \cup \dots \cup (A_1 \times \{a_{2n_2}\}),$$

и

$$|A_1 \times A_2| = \underbrace{|A_1| + \dots + |A_1|}_{n_2 \text{ раз}} = |A_1| \cdot n_2 = |A_1| \cdot |A_2|.$$

Шаг индукции. Пусть уже доказано, что $|A_1 \times \dots \times A_{n-1}| = |A_1| \dots |A_{n-1}|$. Соответствие $((a_1, \dots, a_{n-1}), a_n) \mapsto (a_1, \dots, a_n)$ устанавливает взаимно однозначное отображение между множествами $(A_1 \times \dots \times A_{n-1}) \times A_n$ и $A_1 \times \dots \times A_n$. Применяя базу индукции, получаем:

$$|A_1 \times \dots \times A_n| = |A_1 \times \dots \times A_{n-1}| \times |A_n| = |A_1| \cdot \dots \cdot |A_n|. \quad \square$$

Принципом сложения в комбинаторике называется следующее почти очевидное, хотя и довольно абстрактно формулируемое утверждение.

Теорема 9 (принцип сложения). *Если конечные множества A_i , $1 \leq i \leq n$, попарно не пересекаются (другими словами, не имеют общих элементов), то справедливо равенство*

$$|A_1 \cup \dots \cup A_n| = |A_1| + \dots + |A_n|$$

(словесная формулировка: мощность объединения попарно не пересекающихся множеств равна сумме мощностей этих множеств).

Доказательство. Здесь тоже формально можно провести индукцию по n , но кажется, и так все ясно. $\square$

Для краткости *объединение семейства множеств* A_i , $1 \leq i \leq n$, обозначают еще и так:

$$\bigcup_{i=1}^n A_i.$$

Следующее определение по существу совпадает с определениями, данными Дирихле * и Лобачевским **.

Определение 12. *Отображением (или функцией) $f: A \rightarrow B$ назовем соответствие, при котором каждому элементу множества A сопоставляется ровно один элемент множества B .*

Это определение тесно связано со следующим определением.

Определение 13. Подмножество F множества $A \times B$ назовем *графиком отображения $f: A \rightarrow B$* (обозначение: $F = \Gamma_f$), если для любого элемента a , принадлежащего A , найдется единственный элемент b из B такой, что упорядоченная пара (a, b) принадлежит множеству F .

Этот элемент обозначим $f(a)$ (чтобы подчеркнуть его возможную зависимость от элемента a) и назовем образом элемента a при отображении f .

Примеры. 1. Если $A = \{1, 2, 3, 4, 5, 6, 7, 8\}$, $B = \{a, b, c, d, e, f, g, h\}$, то соответствие

$$\begin{array}{llll} f(1) = a, & f(2) = b, & f(3) = c, & f(4) = d, \\ f(5) = e, & f(6) = f, & f(7) = g, & f(8) = h \end{array}$$

является отображением.

2. Для тех же A, B отображением является соответствие

$$\begin{array}{llll} f(1) = a, & f(2) = a, & f(3) = c, & f(4) = c, \\ f(5) = e, & f(6) = e, & f(7) = g, & f(8) = g. \end{array}$$

Их графики изображаются расстановкой ладей на шахматной доске на рис. 2–3.

А расстановка ладей на рис. 4 не является графиком отображения $f: A \rightarrow B$.

3. Отображение из $\mathbb{N}$ в произвольное множество называется *последовательностью* элементов этого множества.

* П. Лежён Дирихле (Johann Peter Gustav Lejeune Dirichlet, 1805–1859) — знаменитый немецкий математик. Родился во Франции.

** Лобачевский Николай Иванович (1792–1856) — знаменитый русский математик, первооткрыватель неевклидовой геометрии. Ректор Казанского университета в 1827–1846 гг.

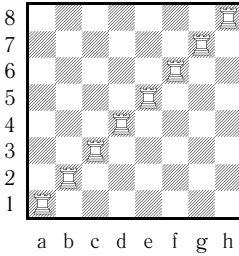


Рис. 2.

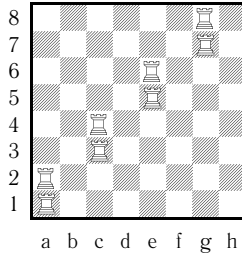


Рис. 3.

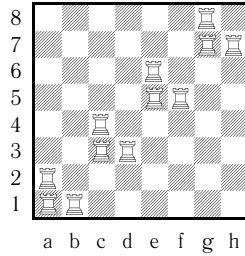


Рис. 4.

Произвольная последовательность обозначается обычно как $\{a_n\}$, где a_n называется ее n -м членом.

Примером последовательности является последовательность Фибоначчи.

Определение 14. Для любого множества M , содержащегося в A , множество $\{f(a): a \in M\}$ образов всех элементов M обозначим $f(M)$ и назовем *образом* множества M .

Для первого отображения предыдущего примера $f(A) = \{a, b, c, \dots, h\}$, а для второго $f(A) = \{a, c, e, g\}$.

Определение 15. Отображение $f: A \rightarrow B$ назовем *наложением*, если $f(A) = B$.

Первое отображение предыдущего примера является наложением, а второе — не является.

Определение 16. Отображение $f: A \rightarrow B$ назовем *вложением*, если разные элементы всегда имеют разные образы.

Первое отображение предыдущего примера является вложением, а второе — нет.

Определение 17. Назовем отображение $f: A \rightarrow B$ *взаимно однозначным отображением*, если отображение f одновременно является и вложением, и наложением.

Первое отображение предыдущего примера взаимно однозначно, а второе — нет.

Примеры. 1. График Γ_f можно изобразить в виде схемы, называемой *двудольным графом*, например, если $A = \{0, 1, 2, 3\}$, $B = \{0, 1, 2\}$, $\Gamma_f = \{(0, 0), (1, 0), (2, 1), (3, 2)\}$, то Γ_f изображается графом с четырьмя вершинами в одной доле и тремя — в другой (рис. 5).

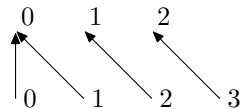


Рис. 5

Отображение f является наложением, но не является вложением. Образом множества $\{0, 1, 2\}$ является множество $\{0, 1\}$.

2. Пример взаимно однозначного отображения

$$A = \{1, 2, 3, 4, 5, 6, 7, 8\} \rightarrow B = \{a, b, c, d, e, f, g, h\}$$

представляет любая расстановка 8 ладей, не угрожающих друг другу.

Следующее определение применимо и к бесконечным множествам.

Определение 18. Если для множеств A и B существует взаимно однозначное отображение $f: A \rightarrow B$, то будем говорить, что A и B имеют *одинаковую мощность*, и записывать это в виде $|A| = |B|$.

Большинство задач перечислительной комбинаторики могут быть сформулированы как задачи о вычислении мощности данного конечного множества.

На использовании понятия равномощности основан следующий прием решения таких задач: если непосредственно мощность множества вычислить не удастся, то пытаются установить взаимно однозначное отображение этого множества с другим множеством, мощность которого уже известна или может быть непосредственно вычислена. Далее мы будем неоднократно пользоваться этим приемом.

Обозначим через $F(A, B)$ *множество всех отображений из A в B* . Имеет место следующая теорема.

Теорема 10. Для любых конечных множеств A и B справедливо равенство $|F(A, B)| = |B|^{|A|}$.

Доказательство. Пусть $A = \{a_1, \dots, a_{|A|}\}$, $B = \{b_1, \dots, b_{|B|}\}$. Существует взаимно однозначное отображение множества $F(A, B)$ на множество $\underbrace{B \times \dots \times B}_{|A|} = B^{|A|}$. Из теоремы 8 следует, что

$$|F(A, B)| = |B^{|A|}| = |B|^{|A|}. \quad \square$$

Обозначим через $\mathcal{P}(A)$ *множество всех подмножеств множества A* (включая само множество A и $\emptyset$ — пустое подмножество). Имеет место следующая

Теорема 11. Для конечного множества A справедливо равенство $|\mathcal{P}(A)| = 2^{|A|}$.

Доказательство. Сопоставим каждому подмножеству M множества A его *индикатор* I_M , т.е. такое отображение $I_M: A \rightarrow \{0, 1\}$, что $I_M(a) = 1$ тогда и только тогда, когда a принадлежит множеству M . Получаем взаимно однозначное отображение $I: \mathcal{P}(A) \rightarrow F(A, \{0, 1\})$. Из теоремы 10 следует, что $|\mathcal{P}(A)| = 2^{|A|}$. $\square$

Кроме функций одной переменной, часто рассматриваются также функции нескольких (иногда говорят — многих) переменных. Например, отображение $f: A^n \rightarrow B$ можно рассматривать как *функцию* $f(x_1, \dots, x_n)$ от n переменных $x_i \in A$, $1 \leq i \leq n$. В частности, если $A = B = \mathbb{R}$, то такую функцию называют *функцией n действительных переменных*.

Примеры. 1. В случае $n = 1$ график такой функции лежит в множестве $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ — двумерном арифметическом пространстве (плоскости).

2. В случае $n = 2$ график такой функции лежит в множестве $\mathbb{R}^2 \times \mathbb{R} = \mathbb{R}^3$ — трехмерном арифметическом пространстве (т. е. является поверхностью).

Для комбинаторики представляют интерес другие классы функций многих переменных.

Определение 19. В случае $A = B = E_2 = \{0, 1\}$ функция $f(x_1, \dots, x_n)$ от n переменных, $x_i \in A$, $1 \leq i \leq n$, называется *функцией двузначной логики*, или *функцией алгебры логики*, а также еще *булевой функцией* *.

В случае $A = B = E_k = \{0, 1, \dots, k-1\}$ функция $f(x_1, \dots, x_n)$ n переменных, $x_i \in A$, $1 \leq i \leq n$, называется *функцией k -значной логики*.

Задачи и упражнения к § 1.6

1. Сколько элементов (вершин) в n -мерном двоичном кубе?
2. Сколько элементов (вершин) в n -мерном k -ичном кубе?
3. Напишите таблицы всех булевых функций от двух переменных.
4. Сколько существует булевых функций от n переменных?
5. Сколько существует функций k -значной логики от n переменных?
6. Сколько различных n -значных чисел можно записать в десятичной системе счисления (первая цифра отлична от 0)?
7. Пусть $n = p_1^{\alpha_1} \dots p_m^{\alpha_m}$. Найдите $\tau(n)$ — число всех натуральных делителей n и $\sigma(n)$ — сумму этих делителей. Докажите, что если $(m, n) = 1$, то $\tau(nm) = \tau(n) \cdot \tau(m)$ и $\sigma(nm) = \sigma(n) \cdot \sigma(m)$.
8. Если p и $2^p - 1$ — простые, то $n = 2^{p-1}(2^p - 1)$ — совершенное число, т. е. такое, что $\sigma(n) = 2n$.

* Дж. Буль (George Boole, 1815–1864) — английский математик и логик, преподавал в Ирландии. Отец писательницы Э.Л. Войнич.

Неизвестно, конечно или бесконечно множество четных совершенных чисел. Самое большое из известных совершенных чисел (и соответственно самое большое из простых чисел Мерсенна*), найденное в 2001 г., получается при $n = 13466917$.

Нечетные совершенные числа до сих пор не найдены.

9. Докажите, что число всех пар подмножеств множества $\{1, 2, \dots, n\}$ таких, что первое из этих подмножеств содержится во втором, равно 3^n .

10. Пусть p — простое число. Сколькими способами можно раскрасить вершины правильного p -угольника, если разрешается использовать заданные k цветов (не обязательно все) и две раскраски, переходящие друг в друга при повороте p -угольника, считаются одинаковыми?

11. Выведите из предыдущей задачи, что p делит $k^p - k$.

12. Произведение 1986 натуральных чисел имеет 1985 различных простых делителей. Докажите, что произведение нескольких из этих чисел либо одно из них являются квадратами натурального числа.

13*. Произведение 48 натуральных чисел имеет 10 различных простых делителей. Докажите, что произведение четырех из этих чисел является квадратом натурального числа.

14*. Произведение 1985 натуральных чисел имеет 9 различных простых делителей.

а) Докажите, что можно выбрать 737 непересекающихся пар чисел, произведения каждых из которых являются квадратами натуральных чисел.

б) Докажите, что можно выбрать 113 непересекающихся четверок чисел так, что произведение каждой четверки будет четвертой степенью натурального числа.

15*. На плоскости нарисованы n точек, занумерованных от 1 до n , и некоторые из них соединены отрезками (ребрами) так, что ребра не пересекаются (по внутренним точкам) и из любой точки можно в любую другую пройти ребрам, причем единственным способом — получилось дерево. Докажите, что ребер в дереве $n - 1$ и число различных деревьев равно n^{n-2} (теорема Кэли**).

У к а з а н и е. Выбрать висячую, т. е. являющуюся концом лишь одного ребра, вершину с наименьшим номером, написать номер второго конца этого ребра, выбросить из дерева это ребро, с оставшимся деревом сделать то же самое и т. д., потом показать, что получившаяся в результате

* О программе поиска новых простых чисел Мерсенна совместными усилиями пользователей Интернета см. www.mersenne.org.

** А. Кэли (Arthur Cayley, 1821–1895) — английский математик. Работая адвокатом в течение 14 лет, опубликовал около 250 математических работ. Оставив адвокатскую практику в 1863 г., стал профессором математики в Кембриджском университете.

последовательность длины $n - 2$ чисел из множества $\{1, \dots, n\}$ однозначно определяет исходное дерево.

§ 1.7. Полиномиальная теорема

Обозначим через $I(A, B)$ множество всех вложений $f: A \rightarrow B$. Другими словами, это число размещений элементов множества A по ящикам, являющимся элементами множества B .

Ясно, что $I(A, B)$ не пусто тогда и только тогда, когда $|A| \leq |B|$.

Определение 20. Число $V \cdot (V - 1) \cdot \dots \cdot (V - n + 1)$ называется *убывающим факториалом* числа V длины n и обозначается $[V]_n$.

Число $V \cdot (V + 1) \cdot \dots \cdot (V + n - 1)$ называется *возрастающим факториалом* числа V длины n и обозначается $[V]^n$.

Упражнение 15. Докажите, что $[-V]_n = (-1)^n [V]^n$, $[-V]^n = (-1)^n [V]_n$.

Теорема 12 (о числе размещений). *Справедливо равенство*

$$|I(A, B)| = |B| \cdot (|B| - 1) \cdot \dots \cdot (|B| - |A| + 1) = [|B|]_{|A|}.$$

Доказательство. Индукция по $|A|$. База ($|A| = 1$) очевидна.

Шаг индукции. Пусть $A = \{1, 2, \dots, n\}$, $B = \{1, 2, \dots, m\}$. Любое отображение f , принадлежащее множеству $I(A, B)$, однозначно определяется, если задать значение $f(n) = i$ из B и отображение f_0 , принадлежащее множеству $I(A_0, B_i)$, где $A_0 = \{1, 2, \dots, n - 1\}$ и $B_i = B \setminus \{i\}$. Таким образом, построено взаимно однозначное отображение из множества $I(A, B)$ в множество

$$\bigcup_{i=1}^m I(A_0, B_i) \times \{i\}.$$

Из предположения индукции и теоремы 9 теперь следует, что

$$|I(A, B)| = m \cdot (m - 1) \cdot \dots \cdot (m - n + 1). \quad \square$$

Определение 21. *Факториалом* числа $V \in \mathbb{N}$ называется произведение $V! = V \cdot (V - 1) \cdot (V - 2) \cdot \dots \cdot 2 \cdot 1$. Для $V = 0$ полагаем $0! = 1$.

Тогда $[V]_n = V! / (V - n)!$ при $V > n \geq 0$.

Теорема 13 (о числе перестановок). *Справедливо равенство*

$$|I(A, A)| = |A| \cdot (|A| - 1) \cdot \dots \cdot 1 = |A|!$$

Доказательство. Утверждение является частным случаем теоремы 12. $\square$

Для краткости вместо $I(A, A)$ пишем $S(A)$.

Определение 22. Элементы множества $S(A)$ называются *перестановками* множества A .

Определение 23. *Перестановкой с повторениями* называется любое слово из множества $\{1, \dots, k\}^n$, в котором каждая «буква» i встречается n_i раз, где $n_1 + \dots + n_k = n$.

Множество всех таких слов обозначим $S(n_1, \dots, n_k)$.

Если имеется n букв ($k=n$), и каждая буква встречается один раз ($n_i=1, i=1, \dots, n$), то $S(1, \dots, 1)$ — это просто множество $S(\{1, 2, \dots, n\})$, элементы которого записаны в виде слова $(a_1, \dots, a_n)$, принадлежащего множеству $\{1, \dots, n\}^n$.

Теорема 14 (о перестановках с повторениями). В обозначениях определения 23 справедливо равенство

$$|S(n_1, \dots, n_k)| = \frac{n!}{n_1! \dots n_k!}.$$

Доказательство. Сопоставим каждому слову w из $S(n_1, \dots, n_k)$ множество всех перестановок из $S_n = S(\{1, 2, \dots, n\})$, которые получаются, если все вхождения каждой буквы i заменить произвольным образом на различные числа из множества $\{l_i, l_i + 1, \dots, l_i + n_i - 1\}$, где $l_i = n_i + \dots + n_{i-1}$. Полученное множество обозначим $S_{n,w}$.

Из теоремы 8 и теоремы 13 вытекает, что $|S_{n,w}| = n_1! \dots n_k!$. Ясно, что

$$S_n = \bigcup_{w \in S(n_1, \dots, n_k)} S_{n,w}$$

— объединение всех множеств $S_{n,w}$, которые попарно не пересекаются, т. е. не имеют общих элементов. Поэтому согласно теореме 9

$$n! = |S_n| = |S(n_1, \dots, n_k)|, \quad \text{откуда} \quad |S(n_1, \dots, n_k)| = \frac{n!}{n_1! \dots n_k!}. \quad \square$$

Упражнение 16. а) Сколько различных слов можно получить, переставляя буквы в слове МАТЕМАТИКА?

б) Сколько различных слов можно получить, переставляя буквы в слове АБРАКАДАБРА?

Перестановка букв в слове называется *анаграммой*.

Упражнение 17. В XVII в. среди ученых существовал обычай объявлять о своих открытиях, нуждающихся в подтверждении, публикацией анаграммы. Галилей, увидев в свою подзорную трубу, что Сатурн имеет по краям какие-то придатки, опубликовал анаграмму

SMAISMRMIELMEPOETALEUMIBUVNEUGTTAVIRAS.

Сколько различных перестановок пришлось бы перепробовать Кеплеру, чтобы разгадать анаграмму Галилея? Напишите точную формулу и оцените число десятичных цифр в изображаемом ею числе.

Из теоремы 14 следует

Теорема 15 (полиномиальная). *Справедливо тождество*

$$(x_1 + \dots + x_k)^n = \sum_{n_1 + \dots + n_k = n} \frac{n!}{n_1! \dots n_k!} x_1^{n_1} \dots x_k^{n_k}.$$

Доказательство. Основной алфавит — $\{x_1, \dots, x_k\}$. Буква x_i входит ровно n_i раз в каждое слово, дающее одночлен $x_1^{n_1} \dots x_k^{n_k}$. $\square$

Определение 24. Число $\frac{n!}{n_1! \dots n_k!}$ обозначается $\binom{n}{n_1, \dots, n_k}$ и называется *полиномиальным коэффициентом*.

Если $k = 2$, то вместо $\binom{n}{n_1, n_2}$ пишут $\binom{n}{n_1}$, ибо $n_2 = n - n_1$, и называют это число *биномиальным коэффициентом*. Вместо $\binom{n}{k}$ используют обычно обозначение C_n^k .

Упражнение 18.

- а) Проверьте, что $C_n^k = [n]_k / k!$.
- б) Проверьте, что справедливо тождество (двойственность биномиальных коэффициентов)

$$C_n^k = \frac{n(n-1) \dots (n-k+1)}{k!} = C_{n-k}^{n-k}.$$

в) Докажите, что последовательность $C_n^0, C_n^1, \dots, C_n^n$ возрастает вплоть до коэффициента $C_n^{\lfloor n/2 \rfloor}$, а с коэффициента $C_n^{\lfloor n/2 \rfloor + 1}$ убывает.

г) Докажите чисто алгебраически *тождество Паскаля*

$$C_{n+1}^k = C_n^k + C_n^{k-1}.$$

Частным случаем полиномиальной теоремы является

Теорема 16 (биномиальная). *Справедливо тождество*

$$(x + y)^n = \sum_{k=0}^n C_n^k x^k y^{n-k}$$

Доказательство. В полиномиальной теореме положим $k=2$. $\square$

Определение 25. Треугольником Паскаля называется таблица

$$\begin{array}{ccccccc}
 & & & & 1 & & & \\
 & & & 1 & & 1 & & \\
 & & 1 & & 2 & & 1 & \\
 & 1 & & 3 & & 3 & & 1 \\
 & \dots & \dots & \dots & \dots & \dots & \dots & \dots
 \end{array}$$

в которой каждая очередная строка на одно число длиннее предыдущей, начинается и заканчивается единицей и каждое из остальных ее чисел равно сумме двух чисел предыдущей строки, между которыми оно находится.

Теорема 17 (о треугольнике Паскаля). В n -й строке треугольника Паскаля стоят в точности биномиальные коэффициенты $C_n^0, C_n^1, \dots, C_n^n$.

Доказательство. Доказательство проводится по индукции. База индукции ($n = 1$) очевидна. Согласно предположению индукции n -я строка треугольника Паскаля состоит из чисел $C_n^0, C_n^1, \dots, C_n^n$. Тогда между числами C_n^{k-1}, C_n^k в $(n+1)$ -й строке будет стоять согласно тождеству Паскаля число $C_{n+1}^k = C_n^{k-1} + C_n^k$. $\square$

Задачи и упражнения к § 1.7

1. Кеплер нашел такое решение анаграммы Галилея (опустив две буквы):

SALVE UMBISTINEUM GEMINAUM MARTIA PROLES

(привет вам, близнецы, Марса порожденье). Он думал, что Галилей открыл спутники Марса. На самом деле они были открыты спустя два века. В действительности Галилей зашифровал фразу (тоже выбросив две буквы)

ALTISSIMUM PLANETAM TERGEMINUM OBSERVAVI

(высочайшую планету тройною наблюдал). Но он ошибся. Вместо придатков у Сатурна оказалось кольцо, которое открыл позднее Гюйгенс. Об этом он тоже опубликовал анаграмму

AAAAAAACCCCCDEEEEGHIIIIILLMMNNNNNNNNNOO
OOPPQRRSTTTTTUUUU.

Сколько различных перестановок пришлось бы перепробовать, чтобы разгадать анаграмму Пойгенса? Напишите точную формулу и оцените число десятичных цифр в изображаемом ею числе.

2. Докажите биномиальную теорему по индукции.
3. Выведите из нее полиномиальную теорему.
4. Если множества A_i попарно не пересекаются и

$$|A_1 \cup \dots \cup A_n| \geq k_1 + \dots + k_n - n + 1,$$

то $|A_i| \geq k_i$ для некоторого i (принцип Дирихле).

5. Если $(n, 10) = 1$, то из одних единиц можно составить число $11\dots 1$, делящееся на n .

6*. Существует число, делящееся на 2^n , десятичная запись которого состоит только из 1 и 2.

7*. Существует число, делящееся на 5^n , десятичная запись которого состоит только из цифр 1, 2, 3, 4, 5.

8*. Если $(n, 5) = 1$, то существует число, делящееся на n , десятичная запись которого состоит только из цифр 1, 2.

9*. Если $(n, 2) = 1$, то существует число, делящееся на n , десятичная запись которого состоит только из цифр а) 1, 2, 3, 4, 5; б) 5, 6, 7, 8, 9; в) только из нечетных цифр.

10*. (С. В. Конягин.) Докажите, что для любого n найдется число, все цифры которого в десятичной записи равны 0, 1, 8, 9, не превосходящее n^4 и делящееся на n .

11. Сколькими способами можно расставить n ладей на шахматной доске $n \times n$ так, чтобы они не били друг друга?

12. Сколькими способами можно разместить n одинаковых шаров по m урнам так, чтобы в каждой урне оказалось не более одного шара?

13. Докажите тождество

$$\sum_{n_1 + \dots + n_k = n} \binom{n}{n_1, \dots, n_k} = k^n.$$

14. Выведите из полиномиальной теоремы, что при простом p и любом натуральном k число $k^p - k$ делится на p (малая теорема Ферма).

15. Если p — простое, большее 5, то число $11\dots 1$, десятичная запись которого состоит из $p - 1$ единицы, делится на p .

16. В классе для каждого $k = 1, \dots, n$ ровно a_k учеников получили не менее k двоек. Сколько всего двоек в этом классе?

17. (Лежандр *.) а) Докажите, что простое число p входит в разложение $n!$ в степени

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \dots + \left\lfloor \frac{n}{p^k} \right\rfloor, \quad \text{где } p^k \leq n < p^{k+1}.$$

б) Докажите, что

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \dots + \left\lfloor \frac{n}{p^m} \right\rfloor + \dots = \frac{n - \nu_p(n)}{p - 1},$$

где $\nu_p(n)$ — сумма цифр p -ичной позиционной записи числа n .

в) Пусть

$$u_k = (p^{k+1} - 1)/(p - 1),$$

$$h = p_m u_m + \dots + p_1 u_1 + p_0, \quad p_m = \lfloor h/u_m \rfloor,$$

$$h_{m-1} = h - p_m u_m, \quad p_{m-1} = \lfloor h_{m-1}/u_{m-1} \rfloor,$$

$$\dots\dots\dots$$

$$h_1 = h_2 - p_2 u_2, \quad p_1 = \lfloor h_1/u_1 \rfloor.$$

Тогда простое p входит в разложение $n!$ в степени h тогда и только тогда, когда

$$n = p_m p^{m+1} + \dots + p_1 p^2 + p_0 p + p',$$

где все p_i и p' суть целые неотрицательные и меньше p .

18. Может ли $n!$ оканчиваться ровно 2004 нулями в десятичной записи?

19. При каких n число $(n-1)!/n$ — целое?

20. Докажите, что число $(2n)!/(n!)^2$ натуральное и делится на $n+1$.

21. Докажите, что $\frac{n!}{a! b! \dots k!}$ — целое, если $a + b + \dots + k \leq n$.

22. Докажите, что число $(2n)!/(n!)^2$ натуральное и делится на $n+1$ и на $2^{\nu_2(n)}$, но не делится на $2^{\nu_2(n)+1}$.

23. Докажите, что число $(2n)!/n!$ делится на 2^n , но не на 2^{n+1} .

24. Докажите, что число $n!/2^n$ — нецелое. При каком натуральном m число $n!/2^{n-m}$ будет целым при всех натуральных n ?

25**. (Чебышёв **.) Выведите из предыдущей задачи, что число $\sqrt[n]{n!}$ не больше произведения по всем простым делителям p числа n сомножителей $p^{1/(p-1)}$, и выведите отсюда, что простых чисел бесконечно много.

* А. М. Лежандр (Adrien Marie Legendre, 1752–1833) — известный французский математик.

** Чебышёв Пафнутий Львович (1821–1894) — выдающийся русский математик, создатель петербургской математической школы.

26.** (Чебышёв.) Докажите, что сумма по всем простым p , не превосходящим n , слагаемых $\lg p/p$ больше, чем $C \lg n$, где C — некоторая константа.

У к а з а н и е. $\sqrt[n]{n!} > n/3$.

27.** (Чебышёв.) Докажите, что сумма по всем простым p , не превосходящим n , слагаемых $1/p$ больше, чем $C \lg \lg n$, где C — некоторая константа.

У к а з а н и е. Если $\mathbb{P}$ — множество всех простых чисел, S — множество всех квадратов, F — множество всех чисел, не делящихся на квадраты, то

$$\left(\sum_{\substack{k=1 \\ k \in S}}^n \frac{1}{k} \right) \cdot \left(\sum_{\substack{k=1 \\ k \in F}}^n \frac{1}{k} \right) \geq \sum_{k=1}^n \frac{1}{k};$$

$$\exp \sum_{\substack{k=1 \\ k \in \mathbb{P}}}^n \frac{1}{k} = \prod_{\substack{k=1 \\ k \in \mathbb{P}}}^n \exp \frac{1}{k} > \prod_{\substack{k=1 \\ k \in \mathbb{P}}}^n \left(1 + \frac{1}{k} \right) \geq \sum_{\substack{k=1 \\ k \in F}}^n \frac{1}{k}.$$

§ 1.8. Сочетания и разбиения

Обозначим через $\mathcal{P}_k(A)$ множество $\{M: M \subset A, |M| = k\}$ всех подмножеств множества A , имеющих мощность k , другими словами, k -подмножеств.

Определение 26. Элементы множества $\mathcal{P}_k(A)$ называются *сочетаниями* элементов из A по k .

Теорема 18 (о числе k -подмножеств). *Справедливо равенство*

$$|\mathcal{P}_k(A)| = C_{|A|}^k.$$

Доказательство. Пусть $A = \{a_1, \dots, a_{|A|}\}$. Сопоставим каждому сочетанию M из $\mathcal{P}_k(A)$ слово $\alpha_1 \dots \alpha_{|A|} \in \{0, 1\}^{|A|}$ такое, что $\alpha_i = 1$ тогда и только тогда, когда элемент a_i принадлежит M . Таким образом, построено взаимно однозначное отображение из множества $\mathcal{P}_k(A)$ в множество $S(k, |A| - k)$. В силу теоремы 14 имеем $|\mathcal{P}_k(A)| = C_{|A|}^k$. $\square$

Теорема 19 (об упорядоченных разбиениях). *Число решений уравнения $x_1 + \dots + x_n = k$ в натуральных числах равно C_{k-1}^{n-1} .*

Доказательство. Сопоставим каждому набору $(x_1, \dots, x_n)$ слово

$$\underbrace{0 \dots 0}_{x_1-1} \underbrace{1 \ 0 \dots 0}_{x_2-1} \dots 1 \dots 1 \underbrace{0 \dots 0}_{x_n-1} \in \{0, 1\}^{k-1}.$$

Таким образом построено взаимно однозначное отображение из множества всех решений уравнения в множество $S(n-1, k-n)$. Остается применить теорему 14. $\square$

Теорема 20 (о разбиениях на неотрицательные слагаемые). Число решений уравнения $x_1 + \dots + x_n = k$ в целых неотрицательных числах равно C_{n+k-1}^{n-1} .

Доказательство. Сопоставим каждому набору $(x_1, \dots, x_k)$ целых неотрицательных чисел набор $(y_1, \dots, y_k)$ натуральных чисел, где $y_i = x_i + 1, i = 1, \dots, k$. Тем самым установлено взаимно однозначное соответствие множества всех целых неотрицательных решений уравнения $x_1 + \dots + x_k = n$ и множества всех решений уравнения $y_1 + \dots + y_k = n + k$ в натуральных числах. Остается применить теорему 19. $\square$

Следствие из теоремы 20. Число слагаемых в полиномиальной формуле равно C_{n+k-1}^{k-1} .

Пример. Сочетания с повторениями появляются при решении следующей задачи имеется kn шаров n различных цветов, по k штук каждого цвета. Сколькими различными способами из них можно выбрать k шаров?

Решение. Каждой выборке сопоставим упорядоченный набор $(x_1, \dots, x_n)$, такой, что $x_1 + \dots + x_n = k$, где x_i — число шаров в выборке, имеющих i -й цвет. Тем самым установлено взаимно однозначное соответствие между числом выборок и числом решений уравнения $x_1 + \dots + x_n = k$ в неотрицательных целых числах. Значит, число выборок, согласно теореме 20, равно $C_{n+k-1}^{n-1} = C_{n+k-1}^k$.

Определение 27. Это число называется числом сочетаний с повторениями из n по k .

Упражнение 19. Проверьте тождество $C_{n+k-1}^k = [n]^k/k!$.

Задачи и упражнения к § 1.8

1. Числовую последовательность назовем монотонной, если каждое следующее число не меньше предыдущего. Докажите, что число монотонных последовательностей длины k , не содержащих чисел отличных от $1, \dots, n$, равно $C_{n+k-1}^k = [n]^k/k!$.

2. Сколькими способами можно разместить n одинаковых шаров по m разным урнам?

3. Вычислите $\sum_{k=0}^{\lfloor n/2 \rfloor} C_n^{2k}$ и $\sum_{k=0}^{\lfloor (n-1)/2 \rfloor} C_n^{2k+1}$.

4. Используя теорему 18, докажите тождество Паскаля

$$C_n^k = C_{n-1}^k + C_{n-1}^{k-1}$$

и тождество Вандермонда *

$$C_m^n = \sum_{k=0}^l C_{m-l}^{n-k} C_l^k.$$

5. Вычислите коэффициент при x^{10} в многочлене $(1+x+x^2)^{10}$.

6. Решите задачу 4, используя биномиальную теорему и тождество $(1+x)^m = (1+x)^l \cdot (1+x)^{m-l}$.

7. Найдите сумму квадратов чисел n -й строки треугольника Паскаля.

8. Докажите тождество для n -го континуанта

$$\underbrace{[x, \dots, x]}_n = \sum_{k=0}^{\lfloor n/2 \rfloor} C_k^{n-k} x^{n-2k}.$$

У к а з а н и е. Можно применить задачу 4 из § 1.4.

9. В треугольнике Паскаля найдите числа Фибоначчи, правда, не в явном виде, а виде суммы чисел по диагоналям.

Докажите, что

$$\sum_{k=0}^n C_{n-k}^k = F_{n+1}.$$

У к а з а н и е. Можно применить предыдущую задачу.

10. Используя тождество Паскаля, докажите, что

$$C_n^k = C_{n-1}^k + C_{n-2}^{k-1} + \dots + C_{n-k}^1 + 1.$$

1						
1	1					
1	2	1				
1	3	3	1			
1	4	6	4	1		
1	5	10	10	5	1	
1	6	15	20	15	6	1

Рис. 6. Диагональ в треугольнике Паскаля

Проверьте, что это равенство верно при $n = k$, если положить $C_m^k = 0$ при $k > m$.

11. Докажите, что многочлен $((x+y)^2 + 3x+y)/2$ осуществляет взаимно однозначное отображение (биекцию) множества $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$ всех упорядоченных пар натуральных чисел на множество $\mathbb{N} = \{0, 1, 2, \dots\}$.

12**. Используя задачу 10, докажите, что многочлен

$$p(x_1, \dots, x_k) = C_{x_1+\dots+x_k+k-1}^k + C_{x_1+\dots+x_{k-1}+k-2}^{k-1} + \dots + C_{x_1+x_2+1}^2 + C_{x_1}^1$$

* А. Вандермонд (Alexandre Théophile Vandermonde, 1735–1796) — французский математик, член Парижской академии наук.

осуществляет биекцию множества $\mathbb{N}^k = \mathbb{N} \times \dots \times \mathbb{N}$ всех наборов натуральных чисел длины k на множество $\mathbb{N} = \{0, 1, 2, \dots\}$. Докажите, что многочлен меньшей степени не может осуществлять такой биекции.

13*. Установите взаимно однозначное соответствие между множеством рациональных чисел и множеством натуральных чисел.

14*. Назовем *цепью* любую строго расширяющуюся последовательность множеств, начинающуюся с $A_0 = \emptyset$ и заканчивающуюся $A_n = \{1, \dots, n\}$. Докажите, что

- а) число всех таких цепей $n!$;
- б) число цепей, в которые входит заданное k -элементное множество, равно $k!(n - k)!$;
- в) число k -элементных подмножеств в $\{1, \dots, n\}$ равно C_n^k (вывести из б)).

15*. (Шпернер *.) Докажите, что если есть семейство попарно не содержащих друг друга подмножеств в $\{1, \dots, n\}$, то их число не превосходит $C_n^{\lfloor n/2 \rfloor}$.

У к а з а н и е. Пусть $\mathcal{U}$ — шпернерово семейство и для любого множества A из семейства $\mathcal{U}$ множество $\mathcal{C}(A)$ состоит из цепей, проходящих через A , тогда для любых множеств A, B из семейства $\mathcal{U}$

$$\mathcal{C}(A) \cap \mathcal{C}(B) = \emptyset$$

и можно применить задачу 14.

16. В классе все учатся на 4 и 5 и никто не учится лучше другого. Какое наибольшее число учеников может быть в классе, если изучаются n предметов?

17*. Индукцией по n докажите формулу включения-исключения **

$$\left| \bigcup_{i=1}^n A_i \right| = \sum_i |A_i| - \sum_{i < j} |A_i \cap A_j| + \sum_{i < j < k} |A_i \cap A_j \cap A_k| - \dots + (-1)^{n-1} |A_1 \cap \dots \cap A_n|.$$

Сколько слагаемых в m -й по счету сумме?

18. (Эйлер.) Используя задачу 17, докажите, что число правильных несократимых дробей со знаменателем n равно $\varphi(n) = n(1 - 1/p_1) \cdot \dots \cdot (1 - 1/p_k)$, где $p_1, \dots, p_k$ — все различные простые делители n .

* Немецкий математик Э. Шпернер доказал эту теорему в 20-е годы XX в.

** Эту формулу первым получил французский математик А. де Муавр (Abraham de Moivre, 1667–1754), проживший почти всю жизнь в Англии.

19. Обозначим $N(n, k)$ число всех отображений из $\{1, \dots, n\}$ в $\{1, \dots, k\}$, являющихся наложениями. Докажите, что

а) $N(n, n) = n!$; б) $N(n, n-1) = C_n^2(n-1)!$;

в) $N(n, k) = k(N(n-1, k-1) + N(n-1, k))$;

г) $N(n, k) = \sum_{j=0}^k (-1)^j C_k^j (k-j)^n$.

У к а з а н и е. Применить задачу 17.

20. План города имеет вид прямоугольника, разбитого улицами на nm одинаковых кварталов. Сколькими способами можно проехать из одного угла города в противоположный угол, преодолев кратчайшее расстояние (см. рис. 7)?

21. Используя задачу 17, решите задачу 4.

22. В каждую клетку шахматной доски размера $n \times n$ запишем число различных кратчайших маршрутов движения ладьи из левого верхнего угла доски до этой клетки. Докажите, что половина доски, лежащая над побочной диагональю, будет заполнена в точности как треугольник Паскаля. Вся же доска целиком будет изображать таблицу, называемую прямоугольником Тартальи* (см. рис. 8).

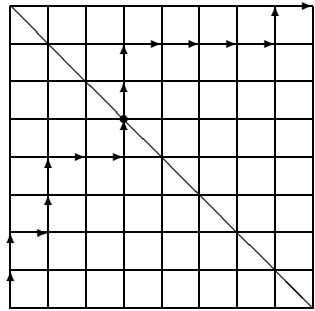


Рис. 7. Один из маршрутов

23. Сколькими способами может попасть на восьмую горизонталь шахматной доски шашка, начинающая движение:

а) из угловой клетки первой горизонтали;

б) из средней клетки первой горизонтали;

в) из средней клетки диагонали доски.

Решите задачу для доски $n \times n$.

24. Введем обозначение $a^{n|h} = a(a-h) \dots (a-(n-1)h)$. Докажите факториальную биномиальную теорему

$$(a+b)^{n|h} = \sum_{k=0}^n C_n^k a^{k|h} a^{(n-k)|h}.$$

1	1	1	1	1	1
1	2	3	4	5	6
1	3	6	10	15	21
1	4	10	20	35	56
1	5	15	35	70	126
1	6	21	56	126	252
1	7	28	84	210	462
1	8	36	120	330	792

Рис. 8. Прямоугольник Тартальи

25. Сколько разных бус можно составить из n различных бусинок?

* Н. Тарталья (Niccolo Tartaglia, ок. 1499–1557) — знаменитый итальянский математик, его имя еще встретится нам в главе IV.

Дополнительные задачи по комбинаторике

1. Сколькими способами можно раскрасить в n цветов вершины куба?

2*. (Эйлер.) Сколькими способами можно разбить выпуклый $(n+2)$ -угольник на треугольники непересекающимися диагоналями?

3*. (Каталан*.) Сколькими способами можно расставить скобки в произведении $(n+1)$ сомножителей?

4*. (Кэли.) Дерево называется бинарным, если из одной его вершины выходит 2 ребра, а из всех невисячих вершин — по 3 ребра. Найдите число различных бинарных деревьев с $n+1$ занумерованной висячей вершиной.

5*. Сколькими способами можно провести шашку из одного угла доски размера $(2n+1) \times (2n+1)$ в соседний угол?

У к а з а н и е. Обозначим координаты углов $(0, 0)$ и $(2n, 0)$ и дополним доску клетками с отрицательными абсциссами, тогда число всех путей из $(0, 0)$ в $(2n, 0)$ равно C_{2n}^n , а число путей, выходящих за край реальной доски, равно числу всех путей из $(0, -2)$ в $(2n, 0)$, т. е. C_{2n}^{n-1} , так как симметрия относительно прямой $x = -1$ переводит начальный отрезок выходящего за край доски пути от $(0, 0)$ до первой клетки с абсциссой -1 в начальный отрезок пути из $(0, -2)$ в $(2n, 0)$.

6*. Докажите, что задачи 2–5 имеют одинаковый ответ: число Каталана

$$C_{2n}^n - C_{2n}^{n-1} = \frac{C_{2n}^n}{n+1}.$$

У к а з а н и е. Установите взаимно однозначное соответствие между множествами из задач 2–5 с помощью рис. 9–11.

На рис. 11 левой скобке соответствует единица, правой — нуль, единице соответствует движение шашки вправо, а нулю — влево.

Положим $\mu(n) = 0$, если n делится на квадрат простого, $\mu(n) = (-1)^k$, если n — произведение k различных простых чисел, и $\mu(1) = 1$ (это так называемая *функция Мёбиуса* **).

7. Докажите, что сумма $\mu(d)$ по всем натуральным d , делящим n , равна 0 при $n > 1$ и равна 1 при $n = 1$.

8*. (Формула Мёбиуса—Чебышёва—Дедекинда***.) Если при любом $x \geq 1$ имеем $g(x) = \sum_{n=1}^{\lfloor x \rfloor} f(x/n)$, то $f(x) = \sum_{n=1}^{\lfloor x \rfloor} \mu(n) g(x/n)$.

* Э. Ш. Каталан (Eugène Charles Catalan, 1814–1894) — бельгийский математик.

** А. Ф. Мёбиус (Augustus Ferdinand Möbius, 1790–1868) — немецкий математик и астроном, изобретатель ленты Мёбиуса.

*** Эта формула была в явном виде опубликована Р. Дедекиндом, а еще раньше — П. Л. Чебышёвым.

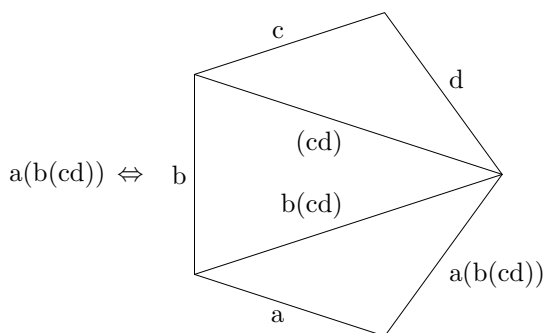


Рис. 9. Триангуляция

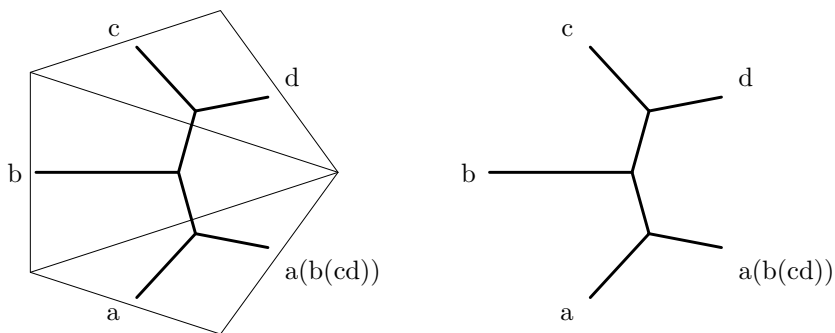


Рис. 10. Триангуляция и дерево

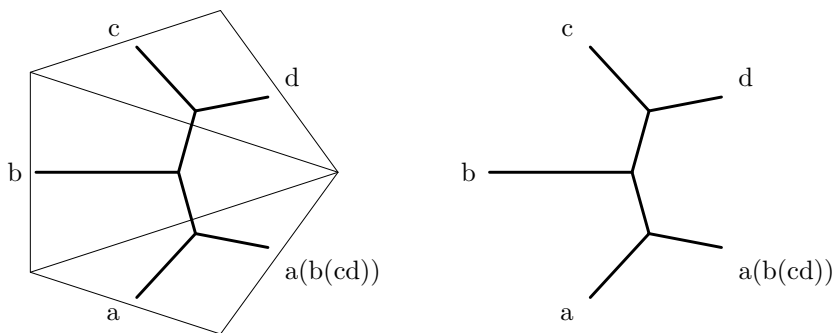


Рис. 11. Дерево, формула, путь шашки и двоичная последовательность

все числа, кроме первого и последнего, кратны заданному простому p тогда и только тогда, когда $n = p^k$.

17. Докажите, что в ряду биномиальных коэффициентов

$$C_n^0, \dots, C_n^k, \dots, C_n^n$$

количество нечетных чисел равно степени двойки.

18. Докажите, что в ряду биномиальных коэффициентов

$$C_n^0, \dots, C_n^k, \dots, C_n^n$$

количество не кратных p чисел равно $(a_1 + 1) \dots (a_m + 1)$, где числа $a_1, \dots, a_m$ — разряды p -ичной записи числа n , а число $m = \lceil \log_p n \rceil$.

19. Докажите, что в первых $p^n - 1$ строках треугольника Паскаля (т.е. среди биномиальных коэффициентов C_n^k , $k \leq m \leq p - 1$) количество не кратных p чисел равно $(p(p+1)/2)^n$.

20. (Люка.) Пусть p — простое, $k \leq n$ — натуральные. Докажите, что

а)* $\text{ord}_p C_n^k = \text{ord}_p C_{np}^{kp}$ и $C_{np}^{kp} - C_n^k$ кратно p ;

б)* $C_n^p - \lfloor n/p \rfloor$ кратно p . Более того, если $\lfloor n/p \rfloor$ кратно p^m , то и C_n^p тоже;

в)** $C_{np+m}^{kp+s} - C_n^k C_m^s$ кратно p при неотрицательных n, m, k, s и при m и s меньших p (биномиальный коэффициент равен нулю, если нижний индекс меньше верхнего, а коэффициент C_0^0 по определению равен 1);

г)** $C_n^k - C_{n_m}^{k_m} \dots C_{n_0}^{k_0}$ кратно p при

$$n = n_m p^m + \dots + n_1 p + n_0, \quad k = k_m p^m + \dots + k_1 p + k_0,$$

$$0 \leq n_i, k_i < p, \quad 0 \leq i \leq m;$$

д)** $C_{p^n-1}^k - (-1)^{\nu_p(k)}$ кратно p ;

е)** $C_{np}^{kp} - C_n^k$ кратно p^2 , а при $p \geq 5$ — кратно и p^3 .

§ 1.9. Перестановки и подстановки

Множество всех перестановок множества $E_n = \{1, 2, \dots, n\}$ обозначим далее S_n .

Произвольную перестановку $\pi \in S_n$ можно представить в виде подстановки

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix}$$

и изобразить с помощью двудольного графа, например, подстановку $\begin{pmatrix} 123 \\ 231 \end{pmatrix}$ можно изобразить как на рис. 12.

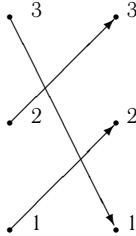


Рис. 12. Граф подстановки

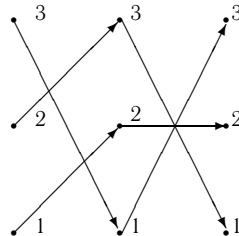


Рис. 13. Умножение подстановок

Слова «перестановка» и «подстановка» для нас по существу будут синонимами.

Определение 28. Если $\pi_1, \pi_2 \in S_n$ — произвольные перестановки, то назовем их *произведением* и обозначим $\pi_1 \circ \pi_2$ такую перестановку $\pi \in S_n$, что для любого i из E_n

$$\pi(i) = \pi_1(\pi_2(i)).$$

Пример. Произведением подстановок $\begin{pmatrix} 123 \\ 231 \end{pmatrix}, \begin{pmatrix} 123 \\ 321 \end{pmatrix}$ является подстановка $\begin{pmatrix} 123 \\ 132 \end{pmatrix}$. В общем случае для умножения подстановки

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \pi_1(1) & \pi_1(2) & \dots & \pi_1(n) \end{pmatrix}$$

на подстановку

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \pi_2(1) & \pi_2(2) & \dots & \pi_2(n) \end{pmatrix}$$

нужно для каждого $i = 1, \dots, n$ выбрать из массива $\{\pi_2(1), \pi_2(2), \dots, \pi_2(n)\}$ (начинаем со второй подстановки!) i -й элемент $\pi_2[i]$, равный, например, j , а потом выбрать из массива $\{\pi_1(1), \pi_1(2), \dots, \pi_1(n)\}$ j -й элемент $\pi_1[j] = \pi_1[\pi_2[i]]$ и поместить его на i -е место в массив $\{\pi(1), \pi(2), \dots, \pi(n)\}$. Всего понадобилось $2n$ операций выборки элемента из массива и n операций записи элемента в массив.

При устных вычислениях достаточно все это проделать при $i = 1, \dots, n - 1$, так как последний элемент результата определяется автоматически.

На рис. 13 изображено умножение подстановок $\begin{pmatrix} 123 \\ 321 \end{pmatrix}, \begin{pmatrix} 123 \\ 231 \end{pmatrix}$.



Порядок, в котором перемножаются перестановки, важен: произведение $\pi_1 \circ \pi_2$ может не совпадать с произведением $\pi_2 \circ \pi_1$.

Упражнение 20. а) Если $\varepsilon \in S_n$ — тождественная перестановка, т. е. $\varepsilon(i) = i$ для любого i из E_n , то для любой перестановки π из S_n

$$\pi \circ \varepsilon = \varepsilon \circ \pi = \pi;$$

б) если $\pi_1 = \begin{pmatrix} 123 \\ 231 \end{pmatrix}$, $\pi_2 = \begin{pmatrix} 123 \\ 132 \end{pmatrix}$, то $\pi_1 \circ \pi_2 = \begin{pmatrix} 123 \\ 231 \end{pmatrix} \neq \begin{pmatrix} 123 \\ 321 \end{pmatrix} = \pi_2 \circ \pi_1$;

в) операция умножения определена для любой упорядоченной пары перестановок, т. е. произведение перестановок — всегда перестановка.

Теорема 21 (об ассоциативности произведения перестановок). Для любых перестановок π_1, π_2, π_3 из S_n справедливо тождество

$$\pi_1 \circ (\pi_2 \circ \pi_3) = (\pi_1 \circ \pi_2) \circ \pi_3.$$

Доказательство. Для любого элемента i из E_n

$$\begin{aligned} (\pi_1 \circ (\pi_2 \circ \pi_3))(i) &= \pi_1((\pi_2 \circ \pi_3)(i)) = \pi_1(\pi_2(\pi_3(i))) = \\ &= (\pi_1 \circ \pi_2)(\pi_3(i)) = ((\pi_1 \circ \pi_2) \circ \pi_3)(i). \quad \square \end{aligned}$$

Графическая иллюстрация напоминает про ассоциативность сложения векторов.

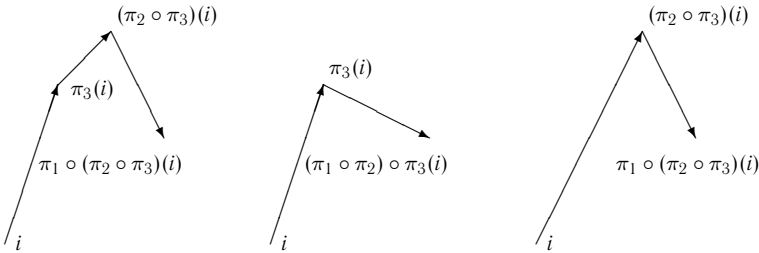


Рис. 14. Ассоциативность умножения подстановок

Упражнение 21. Для любой перестановки π из S_n существует только одна перестановка δ из S_n такая, что $\pi \circ \delta = \varepsilon$, причем $\pi \circ \delta = \delta \circ \pi$.

Для любой перестановки π из S_n обозначим π^{-1} такую перестановку, что $\pi \circ \pi^{-1} = \varepsilon$, где $\varepsilon \in S_n$ — тождественная перестановка.

Графическая иллюстрация: если граф перестановки π отразить симметрично относительно некоторой прямой, отделяющей его доли друг от друга, и направления всех его стрелок изменить на противоположные, то получится граф перестановки π^{-1} .

Определение 29. Эту перестановку назовем *обратной* к π , а операцию: $S_n \rightarrow S_n$, переводящую произвольную $\pi \in S_n$ в $\pi^{-1} \in S_n$, назовем *операцией обращения*.

Пример. Подстановка $\begin{pmatrix} 123456789 \\ 912345678 \end{pmatrix}$ обратна к $\begin{pmatrix} 123456789 \\ 234567891 \end{pmatrix}$.

В общем случае для обращения подстановки

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \pi_1(1) & \pi_1(2) & \dots & \pi_1(n) \end{pmatrix}$$

нужно для каждого $i = 1, \dots, n$ выбрать из массива

$$\{\pi(1), \pi(2), \dots, \pi(n)\}$$

i -й элемент $\pi[i]$, равный, например, j , и поместить число i на j -е место в массив

$$\{\pi^{-1}(1), \pi^{-1}(2), \dots, \pi^{-1}(n)\}.$$

После просмотра всего массива $\{\pi(1), \pi(2), \dots, \pi(n)\}$ будет целиком заполнен и массив

$$\{\pi^{-1}(1), \pi^{-1}(2), \dots, \pi^{-1}(n)\}.$$

Всего понадобилось n операций выборки элемента из массива и n операций записи элемента в массив.

При устных вычислениях достаточно все это проделать при $i = 1, \dots, n - 1$, так как последний элемент результата определяется автоматически.

Упражнение 22. Проверьте, что $(\alpha \circ \beta)^{-1} = \beta^{-1} \circ \alpha^{-1}$ для $\alpha, \beta \in S_n$.

Теорема 22. Для любой перестановки $\pi \in S_n$ справедливо тождество $\pi = (\pi^{-1})^{-1}$. Уравнение $x \circ \pi_1 = \pi_2$ имеет единственное решение $x = \pi_2 \circ \pi_1^{-1}$, а уравнение $\pi_1 \circ x = \pi_2$ — единственное решение $x = \pi_1^{-1} \circ \pi_2$.

Доказательство. Тождество очевидно. Если перестановка x из S такова, что $x \circ \pi_1 = \pi_2$, то

$$x = x \circ \varepsilon = x \circ (\pi_1 \circ \pi_1^{-1}) = (x \circ \pi_1) \circ \pi_1^{-1}.$$

Второе утверждение доказывается аналогично. □

Имеется еще один способ графического изображения перестановок, который получается из первого способа, если отождествить («склеить») все пары соответствующих друг другу вершин из разных долей. Например,

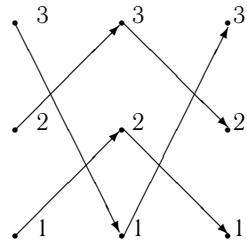


Рис. 15. Обращение подстановок

двудольный граф, соответствующий перестановке

$$\begin{pmatrix} 1234 \\ 2314 \end{pmatrix},$$

превратится в граф, изображенный на рис. 16.

Элементы, которые под действием перестановки π переходят сами в себя, называются неподвижными. На графе им соответствуют вершины с петлями.

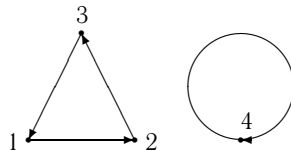


Рис. 16. Граф перестановки

Определение 30. Пусть $a_1, \dots, a_k$ — последовательность различных чисел из E_n . Перестановку π из S_n такую, что $\pi(a_1) = a_2, \dots, \pi(a_{k-1}) = a_k, \pi(a_k) = a_1$, назовем *циклом порядка k* .

Граф этой перестановки содержит $n - k$ петель. Остальные k стрелок (*ребер* графа) вместе с соответствующими им вершинами образуют *подграф*, который называется *циклом длины k* .

Петлю можно считать циклом длины 1. Перестановку π , о которой шла речь, кратко обозначают $(a_1, a_2, \dots, a_k)$. Для того чтобы эта запись имела однозначный смысл, надо указывать, из какого множества S_n взята перестановка π (т. е. указывать число $n = \max_{1 \leq i \leq k} a_i$).

Задачи и упражнения к § 1.9

1. При любой расстановке скобок в произведении $f_1 \circ \dots \circ f_n$ получается одинаковый результат.

2. При $n > 2$ в S_n имеются такие f и g , что $f \circ g \neq g \circ f$.

3. Справедливы тождества

$$(f_1 \circ \dots \circ f_n)^{-1} = f_1^{-1} \circ \dots \circ f_n^{-1}, \quad f \circ g = g \circ f \circ (f^{-1} \circ g^{-1} \circ f \circ g).$$

4. Определим f^n как $f \circ \dots \circ f$ (n раз) при натуральном n , ε при $n = 0$ и $(f^{-1})^{-n}$ при отрицательном целом n . При любых целых числах m, k справедливы тождества

$$f^m \circ f^k = f^{m+k}, \quad (f^m)^k = f^{mk}, \quad (f^m)^{-1} = (f^{-1})^m, \quad (a_1, \dots, a_k)^k = \varepsilon.$$

5. Найдите число всех циклов k -го порядка в S_n .

6. Обозначим через $N(\pi)$ множество всех неподвижных точек перестановки π . Докажите, что если $f, g \in S_n$, $N(f) \cap N(g) = \emptyset$, $N(f) \cup N(g) = E_n$, то $f \circ g = g \circ f$.

7*. Найдите сумму числа неподвижных точек у всех перестановок:

$$\sum_{\pi \in S_n} |N(\pi)|.$$

8. Граф любой перестановки из S_n имеет ровно n ребер (стрелок) и является объединением попарно непересекающихся циклов (в частности, сам может быть циклом длины n).

9*. (И. Н. Сергеев.) Пусть B и A — k -элементные подмножества $E_n = \{1, \dots, n\}$ и $f \in S_n$ — такая перестановка, что для любого i из B справедливо соотношение $i \leq f(i) \in A$. Докажите, что существует перестановка $g \in S_n$ такая, что $j \geq g(j) \notin A$ для любого $j \notin B$ и $j \leq g(j) \in A$ для любого $j \in B$. У к а з а н и е. Примените разбиение на циклы.

10*. На танцевальном вечере в школе на каждом танце разбиение танцующих на пары отличалось от всех встречавшихся ранее, однако каждая пара уже встречалась на одном из первых двух танцев и у стены никто не стоял. Танцы продолжались, пока можно было соблюдать все указанные условия, и прекратились, когда выяснилось, что составить новое разбиение на пары, отличное от встречавшихся ранее, уже нельзя. Докажите, что число всех состоявшихся на вечере танцев равно степени двойки. У к а з а н и е. Примените разбиение на циклы.

11*. (Эйлер.) Письма в n конвертах перемешали так, что ни одно письмо не попало по адресу. Сколькими способами это можно сделать? У к а з а н и е. Примените формулу включения-исключения.

12*. (Преобразование пекаря.) Числа n, m, k таковы, что $k < m < n$ и $(m, n - k) = 1$. В таблице $n \times n$ первая строка заполнена числами $1, 2, \dots, n$, и если в какой-то строке эти числа записаны в порядке $a_1, \dots, a_n$, то в следующей строке они стоят в порядке: $a_{m+1}, \dots, a_n, a_{k+1}, \dots, a_m, a_1, \dots, a_k$. Докажите, что в каждом столбце записаны все числа от 1 до n .

§ 1.10. Циклы и транспозиции

Определение 31. *Транспозициями* называются циклы длины два. Говорят, что циклы $(a_1, \dots, a_k)$ и $(b_1, \dots, b_l)$ *не пересекаются*, если

$$\{a_1, \dots, a_k\} \cap \{b_1, \dots, b_l\} = \emptyset.$$

Справедлива следующая теорема.

Теорема 23 (о разложении на циклы). *Любая перестановка π из S_n может быть представлена в виде произведения попарно непересекающихся циклических перестановок (единичную перестановку $\varepsilon \in S_n$ можно рассматривать как циклическую перестановку порядка 1), причем это представление единственно с точностью до порядка сомножителей, который может быть любым.*

Доказательство. Пусть $\delta_1, \dots, \delta_s$ — попарно непересекающиеся циклические перестановки. Проверим, что если их перемножить в любом порядке, то граф получившейся перестановки является объединением циклов, соответствующих перестановкам δ_i . Остается применить утверждение задачи 8 из § 1.9 и заметить, что разложение графа любой перестановки на циклы единственно. $\square$

Пример. Подстановка $\begin{pmatrix} 123456789 \\ 247138956 \end{pmatrix}$ разлагается на циклы $(1, 2, 4), (3, 7, 9, 6, 8, 5)$, значит,

$$\begin{pmatrix} 123456789 \\ 247138956 \end{pmatrix} = (1, 2, 4)(3, 7, 9, 6, 8, 5) = (3, 7, 9, 6, 8, 5)(1, 2, 4).$$

Опишем в общем случае алгоритм разложения на циклы произвольной подстановки

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix}.$$

Просматриваем по очереди элементы массива $\pi(1)\pi(2) \dots \pi(n)$ и каждый очередной элемент i либо пропускаем, если он был отмечен, либо записываем его в начало очередного формирующегося цикла, после него сразу записываем число $j = \pi(i)$, после него в тот же цикл записываем число $j = \pi(\pi(i))$ и так далее, причем число i и все записываемые в порождаемый им цикл числа j помечаем (например, сменой знака у $\pi(j)$) и продолжаем эту процедуру, пока не будет вычислено число j , совпадающее с i . После этого запись цикла заканчиваем, переходим к очередному элементу массива и применяем к нему ту же процедуру, т. е. пропускаем его, если он оказался уже помеченным, или начинаем с него генерацию нового цикла. Работа заканчивается, когда дойдем до последнего элемента массива. Если он оказался непомеченным, то, очевидно, он порождает тривиальный цикл длины 1.

Одновременно с формированием циклов можно составить еще и список их длин.

Указанный алгоритм использует n операций выборки элемента из массива, столько же операций сравнения очередного выбранного числа с началом формируемого цикла и столько же операций помечивания просмотренных элементов.

Выпишем в невозрастающем порядке длины всех циклов графа перестановки $\pi \in S_n$ (в том числе и петель) и получим вектор $\langle k_1, \dots, k_l \rangle$.

Определение 32. Вектор $\langle k_1, \dots, k_l \rangle$, сумма координат которого равна n , называется *циклическим типом* перестановки π . Если $\langle k_1, \dots, k_l \rangle$ — тип перестановки π , то число $n - l$ называется ее *декрементом* и обозначается $d(\pi)$.

Упражнение 23. Проверьте, что перестановка $\begin{pmatrix} 12345 \\ 31425 \end{pmatrix}$ имеет тип $\langle 4, 1 \rangle$, декремент 3 и является циклом $(1, 3, 4, 2)$.

Определение 33. Пару (i, j) назовем *инверсией* для перестановки π , если $i < j$ и $\pi(i) > \pi(j)$. Число всех инверсий у перестановки π обозначаем $I(\pi)$.

Справедлива следующая теорема.

Теорема 24 (о разложении на транспозиции). (i) Любая перестановка $\pi \in S_n$ разлагается в произведение транспозиций, причем наименьшее число сомножителей в таком произведении равно $d(\pi)$.

(ii) Любая перестановка $\pi \in S_n$ разлагается в произведение вида

$$(1, 2)(2, 3)(3, 4) \dots (n-1, n),$$

причем наименьшее число сомножителей в таком произведении равно $I(\pi)$.

Доказательство. Для него понадобятся две леммы.

Лемма 5. Для любой перестановки $\pi \in S_n$ и транспозиции τ справедливо равенство $|d(\pi \circ \tau) - d(\pi)| = 1$.

Доказательство. Из определения декремента следует, что достаточно проверить, что при умножении перестановки на транспозицию число циклов изменяется на единицу. Будем изображать перестановку π в виде графа, а транспозицию $\tau = (i, j)$ — в виде ребра (i, j) на этом графе. Тогда достаточно проверить, что если ребро соединяет два цикла графа π , то в графе перестановки $\pi \circ \tau$ эти два цикла сливаются в один, а если это ребро соединяет вершины одного цикла, то он распадается на два цикла (остальные циклы в обоих случаях остаются без изменения). Для проверки последнего утверждения достаточно проверить тождества

$$(k_1, \dots, k_l) \circ (m_1, \dots, m_l) \circ (k_l, m_l) = (m_1, m_2, \dots, m_l, k_1, k_2, \dots, k_l),$$

$$(k_1, \dots, k_s, \dots, k_l) \circ (k_s, k_l) = (k_1, \dots, k_s) \circ (k_{s+1}, k_{s+2}, \dots, k_l). \quad \square$$

Лемма 6. Для любой перестановки $\pi \in S_n$ и транспозиции $\tau = (i, i+1)$ справедливо равенство $|I(\pi \circ \tau) - I(\pi)| = 1$.

Доказательство. Непосредственно проверяется, что для обоих перестановок π и $\pi \circ \tau$ число инверсий среди двух пар $\langle k, i \rangle$ и $\langle k, i+1 \rangle$ (при $k < i$) и $\langle i, k \rangle$, $\langle i+1, k \rangle$ (при $k > i+1$) одинаково, а пара $\langle k, l \rangle$ при $\{k, l\} \cap \{i, j+1\} = \emptyset$ для обоих этих перестановок будет или не будет инверсией одновременно. Остается заметить, что пара $\langle i, i+1 \rangle$ будет инверсией ровно для одной из перестановок π и $\pi \circ \tau$. $\square$

Докажем теперь теорему. Пусть $\pi = \tau_1 \dots \tau_k$, где τ_i — произвольные транспозиции (соответственно транспозиции вида $(i, i+1)$). Определим

последовательность перестановок

$$\pi_1 = \pi \circ \tau_k, \quad \pi_2 = \pi_1 \circ \tau_{k-1}, \quad \dots, \quad \pi_k = \pi_{k-1} \tau_1.$$

Тогда

$$\pi_k = \tau_1 \circ \dots \circ \tau_k \circ \tau_k \dots \circ \tau_1 = \varepsilon$$

согласно равенствам $\tau_i^2 = \varepsilon$, и $d(\pi_i) = d(\pi_{i-1}) \pm 1$ согласно лемме 5 (соответственно $I(\pi_i) = I(\pi_i) \pm 1$ согласно лемме 6), а так как $d(\varepsilon) = 0$ (соответственно $I(\varepsilon) = 0$), то $d(\pi) = a - s$, $a + s = k$, $k = d(\pi) + 2s$, где $s \geq 0$ (соответственно $k = I(\pi) + 2s$, $s \geq 0$). Для того чтобы показать, что число s при некотором выборе разложения $\pi = \tau_1 \circ \dots \circ \tau_k$ может равняться нулю, достаточно разложить π на циклы, а циклы на транспозиции согласно лемме 5. В случае разложения на транспозиции вида $(i, i+1)$ обратить s в нуль (и тем самым минимизировать длину разложения k) можно методом, известным в программировании как метод монотонного упорядочения массивов (называемый «всплывтием пузырьков»). Для этого в полученной на предыдущем шаге перестановке π выбираем наибольший из элементов $\pi_j(i)$, еще не стоящий на своем месте, т.е. такой, что $\pi_j(i) > i$, и меняем его с элементом $\pi_j(i+1)$ путем умножения π_j справа на $(i, i+1)$. Тогда у полученной перестановки π_{j+1} число инверсий уменьшается на 1. $\square$

Задачи и упражнения к § 1.10

1. Сколько всего транспозиций в S_n ?
2. Разложите цикл длины k в произведение $k-1$ транспозиций.
3. *Порядок* перестановки π — это минимальное натуральное n такое, что $\pi^n = \varepsilon$.
4. Найдите порядок перестановки $(a_1, \dots, a_k)$.
5. Найдите порядок перестановки $(1, 2) \circ (1, 2, 3) \circ (1, 2, 3, 4, 5, 6)$.
6. Найдите в S_8 все перестановки порядка 15.
7. Найдите все возможные порядки перестановок из S_6 .
8. Сколько в S_n перестановок порядка 2^n ?
9. Какой наивысший порядок у перестановок из S_{10} ?
10. Найдите число всех перестановок в S_n с циклическим типом $\langle m_1, \dots, m_k \rangle$, $m_1 < \dots < m_k$.
- 11*. Найдите число всех перестановок в S_n с циклическим типом $\langle m_1, \dots, m_k \rangle$, $m_1 \leq \dots \leq m_k$.
- 12*. Докажите, что любая перестановка из S_n , имеющая порядок 2, разлагается в произведение не более чем $n/2$ транспозиций.

13. Множество перестановок называется *базисом* в S_n , если любая перестановка разлагается в произведение перестановок из этого множества, а никакое собственное его подмножество этим свойством не обладает. Докажите, что системы транспозиций $\{(1, 2), (1, 3), \dots, (1, n)\}$ и $\{(1, 2), (2, 3), \dots, (n-1, n)\}$, а также транспозиция $(1, 2)$ и цикл $(1, 2, \dots, n)$ являются базисами в S_n .

14*. Сопоставим системе транспозиций $U \subset S_n$ граф с вершинами $1, 2, \dots, n$, в котором вершины i и j соединяются ребром тогда и только тогда, когда транспозиция (i, j) принадлежит множеству U . Докажите, что U — базис в S_n тогда и только тогда, когда соответствующий граф — дерево.

15*. В городе n высотных зданий, никакие три из которых не лежат на одной прямой. Турист, гуляя по городу, записывает порядок, в котором они видны ему из разных районов. Сколько разных перестановок зданий будет в его записях?

16. Для любых перестановок $f, g \in S_n$ справедливо равенство

$$I(f \circ g) \leq I(f) + I(g).$$

17. Назовем *знаком перестановки* $\pi \in S_n$ число $\text{sgn}(\pi) = (-1)^{l(\pi)}$. Докажите, что а) $\text{sgn}(f \circ g) = \text{sgn}(f) \cdot \text{sgn}(g)$; б) $\text{sgn}(\pi) = (-1)^{d(\pi)}$;

$$\text{в) } \text{sgn}(\pi) = \frac{\prod_{i < j} (i - j)}{\prod_{i < j} (\pi(i) - \pi(j))}.$$

18*. Докажите, что знак перестановки из S_n можно определить за Cn операций, где C — константа. У к а з а н и е. Примените пункт б) предыдущей задачи.

19. Перестановку назовем *четной*, если ее знак равен 1. Множество четных перестановок в S_n обозначим A_n . Остальные перестановки назовем *нечетными*. Докажите, что

а) произведение четных перестановок — четно, произведение нечетных перестановок — четно, а произведение четной на нечетную — нечетно;

б) четная перестановка разлагается в произведение всегда четного числа транспозиций, а нечетная — всегда нечетного;

в) порядок нечетной перестановки четен;

г) четных и нечетных перестановок в S_n поровну.

20. Четность перестановки, соответствующей положению маленьких кубиков в кубе Рубика, не меняется при его вращениях.

21*. В игре в пятнадцать нельзя позицию $(1, 2, \dots, 14, 15)$ перевести в позицию $(1, 2, \dots, 13, 15, 14)$.

22*. Множество A_n четных подстановок порождается циклами

а) $(1, 2, 3), (1, 2, 4), (1, 2, 5), \dots, (1, 2, n)$;

б) $(1, 2, 3), (2, 3, 4), \dots, (n-2, n-1, n)$.

23*. Любая четная позиция в игре в пятнадцать может быть получена из начальной позиции $(1, 2, \dots, 14, 15)$.

24*. Испанский король решил перевесить портреты своих предшественников на круглой башне замка. Он хочет за один раз менять местами только два соседних портрета, но лишь в случае, если эти короли не правили сразу друг за другом. Расположения портретов, отличающиеся поворотом круга, он считает одинаковыми. Докажите, что при любом начальном положении портретов можно добиться любого другого их расположения.

25*. Некто, имеющий магнитофон старого образца (не кассетный), получил назад от приятеля свои 12 катушек намотанными в противоположные стороны. Сможет ли он, используя пустую 13-ю катушку, перемотать свои катушки в правильном порядке? Какой будет ответ, если число катушек равняется 11?

26*. В таблице $m \times n$ за один ход разрешается переставить в любом порядке числа любой строки или любого столбца. За какое наименьшее число ходов можно гарантированно получить произвольную заданную перестановку чисел в таблице?

27. Последовательность $\{x_i\}$ из n чисел назовем *k-битонической*, если $x_1 \leq \dots \leq x_k, x_{k+1} \leq \dots \leq x_n$. Докажите, что ее можно переставить в монотонном порядке за Cn операций сравнения чисел и их транспозиции, где C — константа.

28*. (Быстрая сортировка слиянием.) Докажите, что любую последовательность $\{x_i\}$ из n чисел можно переставить в монотонном порядке за $L(n) < Cn \lg n$ операций сравнения чисел и их транспозиции, где C — константа.

У к а з а н и е. Разбейте массив пополам и отсортируйте в монотонном порядке каждую его часть. Тогда за $2L(n/2)$ операций получится $n/2$ -битоническая последовательность, откуда имеем оценку $L(n) \leq 2L(n/2) + Cn$. Если $n \leq 2^k$, то, итерируя это неравенство k раз, находим, что $L(n) \leq Cnk + C_1n \leq C_2n \log_2 n$.

29*. Если последовательность $\{x_i\}$ есть перестановка чисел $1, \dots, n$, то ее можно монотонно отсортировать за Cn операций.

У к а з а н и е. Разложите перестановку на циклы; циклы на транспозиции можно разложить как в задаче 2, используя только $2n$ операций записи в массив, после чего сортировка делается по полученному разложению за n операций транспозиции.

Глава II. Числа и группы

§ 2.1. Группа подстановок

Множество S_n всех перестановок множества E_n , рассматриваемое вместе с операцией умножения перестановок, называем далее *группой перестановок* (или *группой подстановок*).

В дальнейшем будут играть важную роль подмножества группы S_n , замкнутые относительно операций умножения и обращения подстановок. Такие подмножества называются подгруппами группы S_n . Дадим более точное определение.

Определение 34. Подмножество G группы S_n называется *подгруппой*, если вместе с любыми подстановками π и τ оно содержит подстановки π^{-1} и $\pi \circ \tau$ (подразумевается, что множество G не пусто).

Легко доказывается следующая

Теорема 25. Для любой подгруппы G группы S_n выполняются следующие утверждения:

(i) существует элемент $\varepsilon \in G$, для которого при любом элементе π из G

$$\pi \circ \varepsilon = \varepsilon \circ \pi;$$

(ii) для любых элементов π_1, π_2, π_3 из G справедливо равенство

$$\pi_1 \circ (\pi_2 \circ \pi_3) = (\pi_1 \circ \pi_2) \circ \pi_3;$$

(iii) для любого элемента π из G найдется элемент τ из G такой, что

$$\pi \circ \tau = \tau \circ \pi = \varepsilon.$$

Доказательство. (i) В качестве ε можно взять элемент $\pi \circ \pi^{-1}$, где π — произвольный элемент из G .

(ii) Утверждение следует из теоремы 21.

(iii) В качестве элемента τ можно взять π^{-1} . □

Упражнение 24. 1. Множество перестановок $\{\varepsilon, \pi, \pi^2, \dots, \pi^{k-1}\}$ — подгруппа, если k — порядок подстановки π .

2. Множества $\{\varepsilon\}$ и S_n — подгруппы в группе S_n .

Пусть Γ — *граф* с множеством вершин $E_n = \{1, 2, \dots, n\}$. По определению Γ задается множеством неупорядоченных пар $\{i, j\}$, называемых

ребрами графа. Если ребрами графа являются все возможные пары $\{i, j\}$, то граф называется *полным* (несмотря на каламбур) и обозначается K_n .

Определение 35. Перестановка $\pi \in S_n$ называется *самосовмещением графа* Γ , если для любых i, j из E_n пара $\{i, j\}$ является ребром графа Γ тогда и только тогда, когда пара $\{\pi(i), \pi(j)\}$ является ребром графа Γ .

Упражнение 25. а) Множество $G(\Gamma)$, состоящее из всех самосовмещений графа Γ , является подгруппой в S_n .

б) Множество A_n , состоящее из всех подстановок π , принадлежащих S_n , у которых $I(\pi)$ чётно, является подгруппой в S .

Теперь естественно ввести общее понятие группы, которое является одним из самых важных понятий алгебры.

Определение 36. Группой $(G, *)$ называется произвольное множество с операцией $*$: $G \times G \rightarrow G$, которая удовлетворяет следующим условиям, называемым *аксиомами группы*

A1. Существует элемент $e \in G$ такой, что для любого $g \in G$ $g * e = e * g = g$ (такой элемент называют *нейтральным* или *единичным*).

A2. Для любых $g_1, g_2, g_3 \in G$ справедлив закон *ассоциативности*:

$$(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3).$$

A3. Для любого $g \in G$ существует $h \in G$ такой, что $g * h = h * g = e$ (такой элемент называются *обратным* к g и обозначают g^{-1}).

Любая подгруппа группы S_n является группой в смысле этого определения, если в качестве $*$ взять $\circ$ (это утверждает теорема 25). Утверждения теоремы 25 легко доказать и для произвольной группы.

Теорема 26 (о свойствах групповых операций). Любая группа имеет единственный нейтральный элемент и у каждого ее элемента имеется единственный обратный к нему элемент.

Доказательство. Пусть e_1 и e_2 — различные нейтральные элементы. Тогда из A1 следует противоречие: $e_1 = e_1 * e_2 = e_2$.

Пусть элементы h_1 и h_2 — различные обратные к элементу g . Тогда из аксиом A1–A3 следует противоречие:

$$h_1 = h_1 * e = h_1 * (g * h_2) = (h_1 * g) * h_2 = e * h_2 = h_2. \quad \square$$

Доказанная теорема обосновывает применение обозначений: e — для единичного элемента, g^{-1} — для обратного элемента.

Упражнение 26. Проверьте, что

- а) в любой группе G верно, что $e^{-1} = e$;
- б) для любого $g \in G$ справедливо равенство $(g^{-1})^{-1} = g$;
- в) отображение $\varphi_g: G \rightarrow G$, определяемое равенством $\varphi_g(x) = g * x$, является взаимно однозначным отображением.

Произведение $\underbrace{(\dots ((g_1 * g_2) * g_3) * \dots * g_n)}_n$ обозначим через $(g_1 \dots g_n)$.

Упражнение 27. Используя аксиому A2, докажите по индукции, что

$$(g_1 \dots g_n) * (g_{n+1} \dots g_m) = g_1 \dots g_m.$$

Указание. Учесть выполнение равенства $(g_1 \dots g_n) * (g_{n+1} \dots g_m) = ((g_1 \dots g_n) * (g_{n+1} \dots g_{m-1})) * g_m = (g_1 \dots g_{m-1}) * g_m = g_1 \dots g_m$, где предпоследнее равенство следует из предположения индукции.

Пользуясь результатом упражнения, можно показать, что произведение элементов группы не зависит от того, как расставлены в этом произведении скобки (лишь бы порядок элементов в обоих произведениях был одинаков). Например, $(g_1 * g_2) * (g_3 * g_4) = g_1 * ((g_2 * g_3) * g_4)$.

Способ расстановки скобок в произведении далее будем называть формулой. Дадим индуктивное определение формулы.

Определение 37. (i) Выражение вида $\varphi(g_1, g_2) = (g_1 * g_2)$, где g_i — элемент группы $(G, *)$, является *формулой*, построенной из g_1 и g_2 . Эта формула вычисляет элемент из G , равный произведению $g_1 * g_2$.

(ii) Если $\varphi(g_1, \dots, g_n)$ и $\psi(g_{n+1}, \dots, g_m)$ — формулы, построенные из $g_1, \dots, g_n$ и $g_{n+1}, \dots, g_m$ соответственно, то

$$\lambda(g_1, \dots, g_m) = (\varphi(g_1, \dots, g_n) * \psi(g_{n+1}, \dots, g_m))$$

является формулой, построенной из $g_1, \dots, g_m$, и вычисляет элемент группы G , равный произведению элементов, вычисляемых формулами $\varphi(g_1, \dots, g_n)$ и $\psi(g_{n+1}, \dots, g_m)$.

Не требуется, чтобы все g были различны и $n, m - n - 1$ были больше 1; если, например, $n = 1$, то $\varphi(g_1)$ — это просто g_1 .

Упражнение 28. Проверьте, что

- а) $(g_1 * ((g_2 * g_3) * g_4))$ — формула;
- б) $(g_1 * g_2) * g_3 * (g_4 * g_5)$ — не формула.

Теорема 27 (обобщенный закон ассоциативности). Любые две формулы $\varphi(g_1, \dots, g_n)$ и $\psi(g_1, \dots, g_n)$, построенные из элементов $g_1, \dots, g_n$, вычисляют один и тот же элемент. Этот элемент называется *произведением элементов* $g_1, \dots, g_n$ и его (согласно предыдущему утверждению) можно записывать в виде $g_1 * g_2 * \dots * g_n$ без указания скобок, но в указанном порядке.

Доказательство. Доказательство проводится индукцией по n с помощью упражнения 27. Действительно, согласно предположению индукции, элементы, вычисленные формулами φ и ψ , равны соответственно

$$(g_1, \dots, g_k) * (g_{k+1}, \dots, g_n) \quad \text{и} \quad (g_1, \dots, g_e) * (g_{e+1}, \dots, g_n),$$

а согласно упражнению оба этих элемента совпадают с элементом $(g_1, \dots, g_n)$. Шаг индукции обоснован. База индукции ($n = 1, 2$) очевидна. $\square$

Задачи и упражнения к § 2.1

1. Для множества $\mathbb{N}$ с обычной операцией умножения выполнены A1 и A2, но не A3. Такие алгебраические системы называются полугруппами. Проверить, что $\mathbb{Z}$ с операцией обычного умножения и $\mathbb{N} \cup \{0\}$ с операцией обычного сложения — полугруппы.

2. Множество $\mathbb{Q}$ образует группу относительно обычного сложения, а множество $\mathbb{Q} \setminus \{0\}$ относительно умножения. В обеих этих группах операция коммутативна.

3. Найдите группы самосовмещений графов:

а) цикла длины n ;

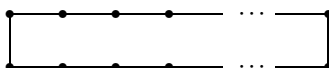


Рис. 17. Цикл

б) цепи длины n ;

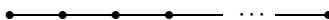


Рис. 18. Цепь

в) трехмерного куба.

4. Найдите группу самосовмещений графа Γ , у которого 10 вершин и 44 ребра.

5*. Найдите дерево с наименьшим числом вершин, имеющее тривиальную группу самосовмещений.

6*. Найдите граф с наименьшим числом вершин, имеющий тривиальную группу самосовмещений.

7. Докажите, что любая подстановка порядка два разлагается в произведение попарно не пересекающихся транспозиций.

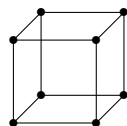


Рис. 19. Трехмерный куб

8*. Докажите, что любой цикл разлагается в произведение двух перестановок порядка два.

У к а з а н и е. Поворот можно разложить в произведение двух осевых симметрий.

9*. Докажите, что любая подстановка разлагается в произведение двух перестановок порядка два.

10*. Найдите все подгруппы групп S_6 и S_4 .

11. Четные перестановки образуют подгруппу в S_n , а нечетные — нет.

12. Множество всех степеней любой подстановки образует подгруппу в S_n .

§ 2.2. Группы и подгруппы

Напомним, что непустое подмножество H группы $(G, \circ)$ называется *подгруппой*, если оно само является группой относительно операции $\circ$.

Для этого необходимо, чтобы для любых элементов g, h из H их произведение $g \circ h$ принадлежало бы H . Любая нетривиальная группа всегда содержит не менее двух подгрупп.

Упражнение 29. Подгруппами группы G являются

- а) единичная подгруппа $\{e\}$;
- б) сама группа G .

Определение 38. Все остальные подгруппы группы G , если они есть, называются *собственным подгруппами*.

Запись $H \leq G$ будет всегда означать, что H — подгруппа группы G . Легко доказывается следующая

Теорема 28 (о подгруппах). *Подмножество H образует подгруппу в группе G тогда и только тогда, когда для любых элементов g, h из H элемент $g \circ h^{-1}$ принадлежит H .*

Д о к а з а т е л ь с т в о. Прямое утверждение ($\Rightarrow$) следует из аксиомы A2 и теоремы 26.

Докажем обратное утверждение ($\Leftarrow$). Пусть g, h — элементы H . Тогда элементы

$$e = h \cdot h^{-1}, \quad h^{-1} = e \cdot h^{-1}, \quad g \cdot h = g \cdot (h^{-1})^{-1}$$

тоже принадлежат подмножеству H .

Аксиомы A1—A3 для множества $(H, \circ)$ выполняются теперь потому, что они выполняются для группы $(G, \circ)$. $\square$



Упражнение 30. Если $H_i \leq G$, $i = 1, \dots, n$, то их пересечение всегда будет подгруппой, но не всегда их объединение будет подгруппой.

Определение 39. Группа G называется *коммутативной*, если произведение в ней не зависит от порядка сомножителей.

Пусть $g \in G$. Обозначим через g^n элемент $\underbrace{g \circ \dots \circ g}_n$, через g^{-n} — элемент $\underbrace{g^{-1} \circ \dots \circ g^{-1}}_n$, т. е. $(g^{-1})^n$; g^0 положим равным e .

Подмножество $\{g^n : n \in \mathbb{Z}\} \subseteq G$ обозначим $[g]$.

Определение 40. Если $g^n = e$, то будем говорить, что n — *период* g . *Наименьший положительный период* элемента g обозначим $t(g)$ и назовем *порядком* элемента g .

Если $g^n \neq e$ при всех $n \neq 0$, то можно положить $t(g) = \infty$.

Справедлива следующая

Теорема 29 (об 1-порожденных подгруппах). *Наименьшая подгруппа, содержащая элемент g , совпадает с $[g]$. Она коммутативна и ее порядок равен $t(g)$. Любой период элемента g делится на его порядок $t(g)$. Если $g^k = g^l$, то $t(g)$ делит $k - l$.*

Доказательство. Если элемент g принадлежит подгруппе $H \leq G$, то из теоремы 28 следует, что подгруппа $[g]$ содержится в подгруппе H . Рассматривая 9 возможных случаев ($m > 0, n > 0$ и т. д.), проверяем равенства $g^n \circ g^m = g^{n+m}$, где n, m — целые числа, а также $(g^n)^{-1} = g^{-n}$, где n — целое число.

Значит, $[g] \leq H$ и группа $[g]$ коммутативна. Пусть $t(g) = \infty$. Тогда $g^n \neq g^m$, если $n \neq m$ (иначе $g^{n-m} = g^n \operatorname{arg}(g^m)^{-1} = e$ и $t(g) < \infty$), и $|[g]| = \infty$. Пусть $t(g) = n > 1$ (если $n = 1$, то $g = e$ и $[g] = e$) и $g^m = e$.

Разделив m на n с остатком, получаем $m = nq + r, 0 \leq r < n, e = g^m = (g^n)^q \circ g^r = g^r$, откуда $r = 0$ (иначе имеем противоречие с определением $t(g)$), т. е. число n делит m .

Поэтому, если $g^k = g^l$, то $g^{k-l} = e$ и число n делит $k - l$, в частности, множества $[g]$ и $\{e, g, \dots, g^{n-1}\}$ равны и все элементы $g^k, 0 \leq k < n$, различны, т. е. $|[g]| = n = t(g)$. $\square$

Теперь легко доказывается следующая

Теорема 30 (о подгруппах конечных групп). *Если группа G конечна и H — такое ее подмножество, что для любых $h, g \in H$ произведение $h \cdot g \in H$, то H — подгруппа группы G .*

Доказательство. Если элемент g принадлежит H , то из теоремы 29 следует, что $|[g]| = n, g^{-1} = g^{n-1} \in [g] \subseteq H$, а из теоремы 28 следует, что $H \leq G$. $\square$

Определение 41. Группа, порождаемая одним из своих элементов (т.е. такая, что все ее элементы являются степенями одного и того же элемента), называется *циклической группой*.

Упражнение 31. Если $(G, *)$ — группа, а g — ее элемент, то $[g]$ — циклическая группа.

Из теоремы 29 следует, что если $(G, *)$ — бесконечная циклическая группа, а $g \in G$ — ее образующий элемент, т.е. $G = [g]$, $G = \{g^n : n \in \mathbb{Z}\}$, то все элементы g^n различны и таблица умножения группы $(G, *)$ задается системой равенств $g^n * g^m = g^{n+m}$, где n, m — целые числа.

Если же $|G| = n$, то из теоремы 29 следует, что

$$G = \{g^k : 0 \leq k \leq n-1\},$$

и таблица умножения группы $(G, *)$ задается системой равенств

$$g^k * g^l = \begin{cases} g^{k+l}, & \text{если } k+l < n, \\ g^{k+l-n}, & \text{если } k+l \geq n. \end{cases}$$

Из сказанного ясно, что любые две циклические группы равных порядков отличаются друг от друга лишь названиями своих элементов; таблицы умножения у этих групп совпадают с точностью до названия строк и столбцов.

На алгебраическом жаргоне предыдущее высказывание произносят так: эти группы *изоморфны*. Дадим точные определения.

Определение 42. Отображение $\varphi: G_1 \rightarrow G_2$, где $(G_1, *)$ и $(G_2, \circ)$ — группы, называется *изоморфизмом* (точнее, *изоморфным отображением* G_1 в G_2), если оно удовлетворяет следующим условиям:

- (i) оно взаимно однозначно;
- (ii) для любых элементов $g, h \in G_1$ справедливо равенство $\varphi(g * h) = \varphi(g) \circ \varphi(h)$.

Упражнение 32. Докажите, что

а) если $\varphi: G_1 \rightarrow G_2$ — изоморфизм, то $\varphi^{-1}: G_2 \rightarrow G_1$ — тоже изоморфизм;

б) тождественное отображение $\varepsilon: G \rightarrow G$ всегда является изоморфизмом;

в) если $\varphi: G_1 \rightarrow G_2$ и $\psi: G_2 \rightarrow G_3$ изоморфизмы, то $\psi \circ \varphi: G_1 \rightarrow G_3$ — также изоморфизм.

Определение 43. Группы $(G_1, *)$ и $(G_2, \circ)$ *изоморфны*, если существует отображение $\varphi: G_1 \rightarrow G_2$, являющееся *изоморфизмом* (обозначение $G_1 \simeq G_2$).

Упражнение 33. Докажите, что а) если $G_1 \simeq G_2$, $G_2 \simeq G_3$, то $G_1 \simeq G_3$; б) если $G_1 \simeq G_2$, то $G_2 \simeq G_1$; в) всегда $G \simeq G$.

Из предыдущего упражнения следует, что множество всех групп распадается на непересекающиеся классы, такие, что любые две группы из одного класса оказываются изоморфными, а группы из разных классов — нет. Все группы из одного класса можно рассматривать как *различные конкретные реализации* одной и той же абстрактной группы.

Например, подгруппа группы S_n , порожденная циклом $(1, 2, \dots, n)$, и множество $\{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ с операцией «+», задаваемой таблицей умножения

$$\bar{a} + \bar{b} = \begin{cases} \overline{a+b}, & \text{если } a+b < n, \\ \overline{a+b-n}, & \text{если } a+b \geq n, \end{cases}$$

представляют из себя циклические группы n -го порядка; они изоморфны.

Вторую из только что упомянутых реализаций циклической группы n -го порядка обозначают $(\mathbb{Z}_n, +)$ и называют группой остатков по модулю n с операцией сложения $(a+b) \bmod n$.

Вообще, в *коммутативных группах* операцию умножения часто обозначают знаком «+» и изменяют терминологию и обозначения, пользуясь следующим словариком:

$(\cdot)$	— умножение;	$(+)$	— сложение;
$(g \cdot h)$	— произведение;	$(g + h)$	— сумма;
(e)	— единица;	(0)	— нуль;
(g^{-1})	— обратный;	$(-g)$	— противоположный;
(g^n)	— степень;	(ng)	— кратное;
$(g \cdot h^{-1})$	— частное;	$(g - h)$	— разность.

Коммутативные группы часто называют *абелевыми* *.

Упражнение 34. Любая бесконечная циклическая группа изоморфна группе $(\mathbb{Z}, +)$ целых чисел с обычной операцией сложения.

С понятием изоморфизма, в сущности, встречаются все школьники, хотя и не всегда осознают это: например, функция $\log_a x$ осуществляет изоморфное отображение группы $(\mathbb{R}_+, \cdot)$ положительных чисел с операцией умножения на группу всех действительных чисел $(\mathbb{R}, +)$ с операцией сложения, так как $\log_a xy = \log_a x + \log_a y$, если $x, y > 0$.



Если в определении изоморфизма забыть про условие взаимной однозначности, то получится определение *гомоморфизма*. Это важное понятие в теории групп, но мы постараемся далее им не пользоваться.

* В честь Н.Х. Абеля (Niels Henrik Abel, 1802–1829) — знаменитого норвежского математика.

Задачи и упражнения к § 2.2

1. Единица (а также минус единица) — образующий элемент в группе $(\mathbb{Z}, +)$.

2. Если $g \in G$, G — группа, $g^n = e$, то порядок g делит n . Если порядок g — простое число, то либо g^m имеет тот же порядок, что и g , либо $g^m = e$.

3. Если H — подгруппа G , $g \in G$, то gHg^{-1} — подгруппа G .

4. Обозначим $Z(G)$ множество всех $g \in G$ таких, что при любом $h \in G$ верно, что $h \cdot g = g \cdot h$ (*центр группы G*). Докажите, что центр группы является подгруппой. Группа G коммутативна тогда и только тогда, когда она совпадает со своим центром.

5. Изоморфное отображение переводит единицу в единицу и обратный элемент — в обратный.



6. Изоморфные группы имеют одинаковые порядки. Обратное неверно.

7. Обозначим $\text{Aut } G$ множество всех перестановок элементов группы G , являющихся изоморфизмами G в себя (такие изоморфизмы называются *автоморфизмами*). Докажите, что $\text{Aut } G$ — подгруппа группы перестановок множества G .

8*. Найдите $\text{Aut } \mathbb{Z}_n$.



9*. Теорема 30 для бесконечных групп неверна.

10. Бесконечная группа имеет бесконечно много подгрупп.

11*. Если порядки всех элементов не больше 2, то группа абелева.

12*. Если порядок группы четен, то некоторый элемент имеет порядок 2.

13*. (Кэли.) Каждая конечная группа изоморфна подгруппе группы подстановок.

14*. Найдите все (с точностью до изоморфизма) полугруппы порядка n , порожденные одним элементом (т. е. циклические).

15*. В любой конечной *полугруппе* (даже без единицы) есть такой элемент g , что $g^2 = g$. Конечная полугруппа будет группой тогда и только тогда, когда такой элемент в ней единственный (единица).

§ 2.3. Циклические группы

В качестве конкретных реализаций циклических групп используем далее $(\mathbb{Z}, +)$ и $(\mathbb{Z}_n, +)$.

Определение 44. Для любого натурального n обозначим $\varphi(n)$ число тех m , которые взаимно просты с n (далее это обозначается

так: $(m, n) = 1$) и удовлетворяют неравенствам $1 \leq m \leq n$. Отображение $\varphi: \mathbb{N} \rightarrow \mathbb{N}$ называется *функцией Эйлера*.

Далее в этой главе часто будет использоваться следующая

Теорема 31 (о циклических группах). (i) Любая подгруппа группы $\mathbb{Z}$ имеет вид $\delta\mathbb{Z} = \{\delta t: t \in \mathbb{Z}\}$, где δ — целое число, а любая подгруппа группы $\mathbb{Z}_n$ — вид $\delta\mathbb{Z}_n = \{\delta t: 0 \leq t < n/\delta\}$, где δ делит n .

(ii) Подгруппы циклической группы цикличны. Все подгруппы бесконечной циклической группы $\mathbb{Z}$ (кроме тривиальной подгруппы $\{0\}$) изоморфны ей самой. Порядок любой подгруппы конечной циклической группы $\mathbb{Z}_n$ является делителем n и для любого t , делящего n , имеется ровно одна подгруппа порядка t . Общее число всех подгрупп в группе $\mathbb{Z}_n$ равно $d(n)$ — числу всех делителей числа n и все эти подгруппы попарно неизоморфны.

(iii) Для любого элемента $\bar{a} \in \mathbb{Z}_n$ его порядок $t(\bar{a})$ равен $\frac{n}{(a, n)}$ и совпадает с порядком порожденной им группы $[\bar{a}]$. Число всех элементов $\bar{a} \in \mathbb{Z}_n$, у которых $t(\bar{a}) = t$, равно $\varphi(t)$.

(iv) Образующими группы $\mathbb{Z}$ являются элементы $a = \pm 1$ и только они. Элемент $\bar{a}$ порождает всю группу $\mathbb{Z}_n$ тогда и только тогда, когда его порядок $t(\bar{a}) = n$, а последнее справедливо тогда и только тогда, когда $(a, n) = 1$. Число образующих в группе $\mathbb{Z}_n$ равно $\varphi(n)$.

(v) Для любого $t \in \mathbb{Z}$ множество $t\mathbb{Z}_n = \{\bar{a}: \bar{a} = t\bar{b}, \bar{b} \in \mathbb{Z}_n\}$ состоит из $\frac{n}{(t, n)}$ элементов.

Доказательство. Пусть $H \leq \mathbb{Z}_n$. Если $H = \{0\}$, то $H = n \cdot \mathbb{Z}_n$. Если $\{0\} \neq H$, то пусть δ — наименьшее число такое, что $\bar{\delta} \in H \setminus \{0\}$ (оно существует в силу принципа индукции). Тогда $H = \delta\mathbb{Z}_n$. Действительно, если бы существовал элемент $\bar{a} \in H \setminus \delta\mathbb{Z}_n$, то, деля a на δ с остатком, мы бы получили, что $\bar{r} = \overline{a - \delta q} \in H$, где q — частное, r — остаток, так как

$$\bar{r} = \overline{a - \delta q} = \bar{a} + q(\overline{-\delta}) = \bar{a} + q(\overline{n - \delta}), \quad \bar{a} \in H, \quad \overline{n - \delta} = -\bar{\delta} \in H,$$

$0 < r < \delta$, а это противоречит определению δ . Поэтому $H \leq \delta\mathbb{Z}_n$, а так как $\bar{\delta} \in H$, $\delta\mathbb{Z}_n \leq [\bar{\delta}]$, то согласно теореме 29 имеем $\delta\mathbb{Z}_n = H = [\bar{\delta}]$.

Равенство $\delta\mathbb{Z}_n = \{\delta t: 0 \leq t < n/\delta\}$ следует из того, что $\delta \mid n$ (если δ не делит n , то, заменяя a на n в уже проведенном рассуждении, получим противоречие).

Пусть $H \leq \mathbb{Z}$. Если $H = \{0\}$, то $H = 0 \cdot \mathbb{Z}$. Если $\{0\} \neq H$, то рассуждением, аналогичным уже приведенному, получим, что $H = \delta \cdot \mathbb{Z} = (-\delta) \cdot \mathbb{Z}$, где $\delta \in \mathbb{N}$. Утверждение (i) доказано.

Утверждение (ii) следует из того, что отображения $x \rightarrow x \cdot \delta$ и $\bar{x} \rightarrow \overline{x \cdot \delta}$ являются изоморфизмами между $\mathbb{Z}$ и $\delta\mathbb{Z}$ и между $\mathbb{Z}_n$ и $\delta\mathbb{Z}_n$ соответственно

(последнее при $(\delta, n) = 1$), а отображение $\delta \rightarrow \delta \cdot \mathbb{Z}_n$ устанавливает взаимно однозначное соответствие между делителями числа n и подгруппами группы $\mathbb{Z}_n$.

Докажем утверждения (iii) и (iv). Пусть $t(\bar{a}) = m$. Согласно (i) имеем $[\bar{a}] = \delta \mathbb{Z}_n$, $\delta \mid n$, а так как $\bar{a} \in \delta \mathbb{Z}_n$, то $\delta \mid a$, откуда $\delta \geq (a, n)$. Но $\bar{a} \in (a, n) \mathbb{Z}_n$, значит, $[\bar{a}] \leq (a, n) \mathbb{Z}_n$, поэтому

$$m = t(\bar{a}) = \frac{n}{\delta} \leq \frac{n}{(a, n)} \leq \frac{n}{\delta},$$

следовательно,

$$m = \frac{n}{\delta} = \frac{n}{(a, n)} = t(\bar{a}) = [\bar{a}].$$

В частности, видим, что $[\bar{a}] = \mathbb{Z}_n$ тогда и только тогда, когда $n = |[\bar{a}]| = t(\bar{a}) = \frac{n}{(a, n)}$, другими словами, когда $(a, n) = 1$, откуда также следует, что

$$|\{\bar{a}: [\bar{a}] = \mathbb{Z}_n\}| = |\{a: 1 \leq a \leq n, (a, n) = 1\}| = \varphi(n).$$

Далее (согласно (ii)), $t(\bar{a}) = m$ тогда и только тогда, когда $|[\bar{a}]| = m$, другими словами, когда $[\bar{a}] = \frac{n}{m} \mathbb{Z}_n \simeq \mathbb{Z}_m$. Применяя полученную формулу для $|\{a: [\bar{a}] = \mathbb{Z}_n\}|$, имеем

$$\begin{aligned} |\{\bar{a}: \bar{a} = \mathbb{Z}_n, t(\bar{a}) = m\}| &= |\{\bar{a}: \bar{a} \in \frac{n}{m} \mathbb{Z}_n, [\bar{a}] = \frac{n}{m} \mathbb{Z}_n\}| = \\ &= |\{\bar{b}: \bar{b} \in \mathbb{Z}_m, [\bar{b}] = \mathbb{Z}_m\}| = \varphi(m). \end{aligned}$$

Так как тот факт, что $[a] = \mathbb{Z}$ тогда и только тогда, когда $a = \pm 1$, очевиден, то утверждения (iii) и (iv) доказаны.

Докажем последнее утверждение. Согласно (i) $m \mathbb{Z}_n = \delta \mathbb{Z}_n$, ведь $m \mathbb{Z}_n \leq \mathbb{Z}_n$. Отсюда $\delta \mid m$ (поскольку $m \in m \mathbb{Z}_n = \delta \mathbb{Z}_n$), а так как $\delta \mid n$, то $\delta \leq (m, n)$. Но при любом $\bar{a} \in \mathbb{Z}_n$ имеем $\frac{n}{(m, n)} \cdot m \bar{a} = \frac{m}{(n, m)} (n \cdot \bar{a}) = 0$. Значит, согласно теореме 29 имеем $\frac{n}{\delta} = |\delta \mathbb{Z}_n| \leq \frac{n}{(m, n)}$, т.е. $\delta \geq (m, n)$ и поэтому $\delta = (m, n)$, следовательно,

$$|m \mathbb{Z}_n| = |\delta \mathbb{Z}_n| = \frac{n}{\delta} = \frac{n}{(m, n)}. \quad \square$$

Из доказанной теоремы выведем еще одну теорему.

Теорема 32 (о линейном представлении НОД). Пусть $a_1, \dots, a_n$ — целые числа, $(a_1, \dots, a_n)$ — их наибольший общий делитель. Тогда найдутся целые числа x_i , для которых

$$(a_1, \dots, a_n) = x_1 a_1 + \dots + x_n a_n.$$

Доказательство. Рассмотрим в группе $\mathbb{Z}$ подгруппу

$$[a_1, \dots, a_n] = \{a \in \mathbb{Z} : a = a_1x_1 + \dots + a_nx_n, x_i \in \mathbb{Z}, i = 1, \dots, n\}.$$

Согласно теореме 31 $[a_1, \dots, a_n] = d\mathbb{Z}$, где d — натуральное число ($d = 0$ лишь когда $a_i = 0, i = 1, \dots, n$). Так как $a_i \in [a_1, \dots, a_n]$, то $a_i \in d\mathbb{Z}$, значит, $d \mid a_i, i = 1, \dots, n$.

Пусть число δ также удовлетворяет условиям $\delta \mid a_i, i = 1, \dots, n$. Тогда $a_i \in \delta\mathbb{Z}, i = 1, \dots, n$, откуда $[a_1, \dots, a_n] \subseteq \delta\mathbb{Z}$, т. е. $d\mathbb{Z} \subseteq \delta\mathbb{Z}$, значит, $d \in \delta\mathbb{Z}$ и $\delta \mid d, |\delta| \leq d$, таким образом, d действительно равно НОД($a_1, \dots, a_n$). Так как d принадлежит множеству $d\mathbb{Z} = [a_1, \dots, a_n]$, то $d = a_1x_1 + \dots + a_nx_n$, где x_i — целые числа, $i = 1, \dots, n$. $\square$

Приведенное рассуждение также доказывает, что НОД($a_1, \dots, a_n$) делится на любой общий делитель этих чисел, и уравнение

$$a_1x_1 + \dots + a_nx_n = a$$

разрешимо в целых числах тогда и только тогда, когда НОД($a_1, \dots, a_n$) делит a .

В частности, если $(a, b) = 1$, то $ax + by = 1$ при некоторых целых x, y . Другое доказательство этого факта было ранее получено с помощью алгоритма Евклида.

Задачи и упражнения к § 2.3

1. Выведите из теоремы 32 все утверждения задачи 5 из § 1.2, а также следующие утверждения:

- (i) $[ka, kb] = k[a, b]$;
- (ii) $(a, b) = (a \pm b, [a, b])$;
- (iii) если $\delta \mid a, \delta \mid b$, то $(a/\delta, b/\delta) = (a, b)/\delta$;
- (iv) $[a_1, \dots, a_n] = a_1 \cdot \dots \cdot a_n / (A_1, \dots, A_n)$, $A_i = a \cdot \dots \cdot a_n / a_i$;
- (v) $[a_1, \dots, a_n] = [a_1, [a_2, \dots, a_n]]$;
- (vi) $((a_1, \dots, a_n)) = (a_1, (a_2, \dots, a_n))$;
- (vii) если $a_i \mid b$, то $[a_1, \dots, a_n] \mid b$;
- (viii) если a делит bc , то $a/(a, b)$ делит c ;
- (ix) если p — простое, $p \mid a_1 \cdot \dots \cdot a_n$, то $p \mid a_i$ при некотором i .

2. Используя предыдущее утверждение, докажите теорему 4 из § 1.2.

3. Докажите, что $d(n) \leq 2\sqrt{n}$.

4*. (Гаусс.) Докажите, что $\sum_{d \mid n} \varphi(d) = n$.

5. Решите уравнение $15x - 9y = 6$ в области $\mathbb{Z}$.

6. Решите систему $(x, y) = 15, [x, y] = 840$.

7. Нарисовать диаграмму включений семейства всех подгрупп группы $\mathbb{Z}_{60}$.

8*. Множество $M \subseteq \mathbb{N}$ называется *полугруппой* (без единицы), если для любых $x, y \in M$ их сумма $x + y$ также принадлежит M . Докажите, что любая такая полугруппа *конечно порожденная*, т. е. $M = \{a: a = a_1x_2 + \dots + a_nx_n, x_i \in \mathbb{N}\}$ при некоторых натуральных a_i .

9*. Имеется несколько карточек с числами. Для любого $n \leq 2004$ имеется ровно n карточек, на которых написаны его делители. Докажите, что любое $n \leq 2004$ написано хотя бы на одной карточке.

У к а з а н и е. Примените задачу 4.

§ 2.4. Теорема Лагранжа

Пусть G — группа, H — ее подгруппа.

Определение 45. Множество $gH = \{gh: h \in H\}$ называется (*левым*) *смежным классом* по подгруппе H , содержащим элемент g (действительно, $g = ge \in gH$).

Правым смежным классом называется множество $Hg = \{hg: h \in H\}$.

Если группа G коммутативна, то всегда $gH = Hg$.

Далее рассматриваем только левые смежные классы. Справедлива следующая

Лемма 7. *Любые два смежных класса по подгруппе H либо не пересекаются, либо совпадают.*

Доказательство. Пусть, например, $aH \cap bH \neq \emptyset, c \in aH \cap bH$. Тогда $c = ah_1 = bh_2$, где $h_i \in H$ и

$$aH = a(h_1H) = (ah_1)H = cH = (bh_2)H = b(h_2H) = bH.$$

При выводе этой цепочки равенств мы пользовались ассоциативностью и равенством $hH = H$, где h — элемент H , которое проверяется следующим образом.

Для любого элемента h' из H произведение $h'h$ принадлежит H и поэтому hH — подмножество в H .

Любой элемент h'' из H можно представить в виде $h'' = h(h^{-1}h'')$, откуда видно, что он принадлежит также hH , и поэтому H содержится в hH . Доказанные включения и означают, что $H = hH$. $\square$

Нам понадобится также

Лемма 8. *В любом смежном классе по H столько же элементов, сколько и в H .*

Доказательство. Действительно, отображение $\varphi: H \rightarrow gH$, определяемое равенством $\varphi(x) = gx$, является взаимно однозначным (упражнение 26 из § 2.1). $\square$

Теорема 33 (Лагранж *). *Порядок конечной подгруппы всегда является делителем порядка соответствующей группы.*

Доказательство. Пусть G — группа, H — ее подгруппа. Обозначим через $[G : H]$ число всех попарно различных смежных классов gH , $g \in G$ и пусть $g_1H, \dots, g_mH$ — список всех этих классов, $m = [G : H]$.

Из леммы 7 следует, что $g_iH \cap g_jH = \emptyset$, если $i \neq j$. Методом от противного докажем, что

$$\bigcup_{i=1}^m g_iH = G.$$

Пусть найдется элемент $g_{m+1} \in G$ такой, что

$$g_{m+1} \notin \bigcup_{i=1}^m g_iH.$$

Тогда согласно лемме 7 класс $g_{m+1}H$ отличен от классов g_iH , $i = 1, \dots, m$, так как

$$g_{m+1} \in g_{m+1}H, \quad g_{m+1} \notin g_iH, \quad i = 1, \dots, m.$$

Получается противоречие с определением списка g_iH , $i = 1, \dots, m$. Согласно лемме 8, имеем $|g_iH| = |H|$, $i = 1, \dots, m$, поэтому из равенств

$$m = [G : H], \quad \bigcup_{i=1}^m g_iH = G,$$

соотношения $g_iH \cap g_jH = \emptyset$, $i \neq j$, и комбинаторного принципа сложения следует равенство $[G : H] = |G|/|H|$, означающее, что $|G|$ делится на $|H|$. $\square$

Определение 46. Число $[G : H] = |G|/|H|$ называется *индексом* подгруппы H в группе G .

Если группы G и H не обязательно конечны, то $[G : H]$ — это число смежных классов в группе G по подгруппе H .

З а м е ч а н и я. Если $K \leq H \leq G$, то $[G : K] = [G : H] \cdot [H : K]$, в том смысле, что если $[G : K]$ конечно, то $[G : H]$, $[H : K]$ тоже конечны и справедливо упомянутое равенство; оно также справедливо, если конечны $[G : H]$, $[H : K]$.

* Ж.Л. Лагранж (Joseph Louis Lagrange, 1736–1813) — великий французский математик и механик.

Сформулированное утверждение обобщает теорему Лагранжа. Его доказательство основано на том, что любая (не только конечная) группа G представляется в виде объединения всех различных смежных классов по подгруппе H , причем эти классы попарно не пересекаются, а их число (если оно конечно) равно $[G : H]$.

Отметим, что в предыдущих рассуждениях вместо левых смежных классов можно с тем же успехом использовать правые.



Левые смежные классы, вообще говоря, не совпадают с правыми.

Определение 47. Если при любом $g \in H$ выполняется $gH = Hg$, то подгруппа H называется *нормальной*. Если H нормальна в G , то это обозначается $H \triangleleft G$.



Равенство $gH = Hg$ не означает, что при любом $h \in H$ обязательно $gh = hg$, оно лишь означает совпадение множеств $\{gh : h \in H\}$ и $\{hg : h \in H\}$.

Упражнение 35. Равенство $gH = fH$ справедливо тогда и только тогда, когда $gf^{-1} \in H$.

Будем говорить, что *сравнение* $a \equiv_H b$ справедливо тогда и только тогда, когда $ab^{-1} \in H$ (или тогда и только тогда, когда $aH = bH$, что равносильно). Введенное отношение между элементами группы G называется (левой) *сравнимостью* по подгруппе H . Аналогично вводится *правая сравнимость*.

Упражнение 36. Левая и правая сравнимости по подгруппе H совпадают тогда и только тогда, когда $H \triangleleft G$.

Упражнение 37. Если группа G коммутативна, то $H \leq G$ тогда и только тогда, когда $H \triangleleft G$. Обратное неверно.

Определение 48. Число t называется *периодом* группы G , если для любого $g \in G$, $g^t = e$. *Наименьший положительный период* группы G обозначим $t(G)$.

Теорема 34 (малая теорема Ферма для групп). (i) Число t является периодом группы G тогда и только тогда, когда $t(G)$ делит t .

(ii) Если группа G конечна, то $t(G)$ равен НОК порядков всех элементов $g \in G$.

(iii) Порядок любого элемента является делителем порядка группы.

(iv) Порядок группы является ее периодом.

Доказательство. Пункт (i) докажем методом от противного.

Пусть t — период группы G , $t = t(G)q + r$, q — натуральное число, $0 < r < t(G)$. Так как для любого $g \in G$ выполняется

$$e = g^t = (g^{t(G)})^q g^r = e^q g^r = g^r,$$

значит, r — положительный период G , меньший $t(G)$, чего не может быть.

Докажем пункт (ii). Если t — период G , то для любого $g \in G$ имеем $g^t = e$, значит, t делится на $|[g]|$, откуда следует, что $\text{НОК}\{|[g]| : g \in G\}$ делит t . Теперь утверждение (ii) следует из утверждения (i).

Докажем пункт (iii). Пусть g — элемент группы G . Так как его порядок равен порядку порожденной им группы $[g]$, а $[g] \leq G$, то согласно теореме 33 порядок $|G|$ делит $|[g]|$, что и требовалось.

Последний пункт следует из двух предыдущих. $\square$

Следствие из теоремы 34. Для любого элемента g произвольной группы G его порядок равен минимальному периоду $t([g])$ порожденной им подгруппы $[g]$.

Теорема 35 (о циклических группах простого порядка). Группа G не имеет собственных подгрупп тогда и только тогда, когда она циклическая простого порядка. Любая группа простого порядка циклическа.

Доказательство. Тот факт, что группа простого порядка не имеет собственных подгрупп, следует из теоремы Лагранжа. Если же группа не имеет собственных подгрупп, то, согласно теореме 29, она циклическая, а согласно теореме 31 — простого порядка. $\square$

Далее появятся и другие применения теоремы 33.

Задачи и упражнения к § 2.4

1. Найдите период группы S_4 .
2. Если $|G : H| = 2$, то $H \triangleleft G$ и H — одна из наибольших из подгрупп G .
3. Найдите наибольшую подгруппу в S_n .
4. Проверить, что всегда:
 - а) $a \equiv_H a$;
 - б) $a \equiv_H b \Rightarrow b \equiv_H a$;
 - в) $a \equiv_H b, b \equiv_H c \Rightarrow a \equiv_H c$.
5. Если $G = \mathbb{Z}$, $H = m\mathbb{Z}$, то вместо $a \equiv_H b$ будем писать $a \equiv b \pmod{m}$. Докажите, что:
 - а) $a \equiv b \pmod{m}$ тогда и только тогда, когда $m \mid a - b$ и тогда и только тогда, когда a и b равноостаточны при делении на m ;

- б) $a \equiv b \pmod{m} \Rightarrow a^m \equiv b^m \pmod{m}$;
 в) $a \equiv b \pmod{m}, c \equiv d \pmod{m} \Rightarrow a + c \equiv b + d \pmod{m}$,
 $ac \equiv bd \pmod{m}$;
 г) $a \equiv b \pmod{m} \Rightarrow ka \equiv kb \pmod{m}$;
 д) $ka \equiv kb \pmod{m}, (k, m) = 1 \Rightarrow a \equiv b \pmod{m}$;
 е) $a \equiv b \pmod{m}, \delta = (a, b, m) \Rightarrow a/\delta \equiv b/\delta \pmod{m/\delta}$;
 ж) $a \equiv b \pmod{m_i}, i = 1, \dots, n \Rightarrow a \equiv b \pmod{[m_1, \dots, m_n]}$.

6. Докажите, что:

- а) $a^k \equiv b^k \pmod{|a - b|}, a \neq b$;
 б) $a^{2k} \equiv b^{2k} \pmod{|a + b|}, a \neq b$;
 в) $a^{2k+1} \equiv -b^{2k+1} \pmod{|a + b|}, a \neq b$.

7. Докажите сравнения:

- а) $a_0 + a_1 10 + \dots + a_n 10^n \equiv a_0 + a_1 + \dots + a_n \pmod{9}$;
 б) $a_0 + a_1 10 + \dots + a_n 10^n \equiv a_0 - a_1 + \dots \mp a_n \pmod{11}$.

8. Решите сравнение $27x \equiv 6 \pmod{51}$.

9. Найдите с точностью до изоморфизма все группы порядка не выше 6 и все нормальные подгруппы в них.



Теорема, обратная к теореме Лагранжа, неверна.

10. Докажите, что группа четных перестановок в S_4 изоморфна группе вращений тетраэдра, имеет порядок 12, но не имеет подгрупп порядка 6 (контрпример к обращению теоремы Лагранжа).

11. На множестве всех подмножеств данного n -элементного множества определим операцию *симметрической разности* множеств: $A \triangle B = (A \setminus B) \cup (B \setminus A)$. Докажите, что это множество образует группу относительно введенной операции. Докажите, что ее порядок и порядок любой ее подгруппы равен степени двойки.

12. В военкомате занимаются составлением списков призывников. В конце года оказалось, что для каждого двух составленных списков A и B был составлен еще список C , в котором записаны все призывники, входящие только в один из списков A и B , но не в оба сразу. Докажите, что число составленных списков на единицу меньше степени двойки.

13*. Докажите, что группа A_5 четных подстановок не имеет нетривиальных нормальных делителей (такие группы называют *простыми*).

14*. В Москве 18**** телефонных номеров («*» означает неизвестную цифру). Докажите, что найдутся два номера, сумма которых (рассматриваемых как числа в десятичной записи) оканчивается на семизначное число, не являющееся московским номером (на телефонную книгу не ссылаться).

15. Если $H \triangleleft G$, $a \equiv_H b$, $c \equiv_H d$, то $ac \equiv_H bd$. Без предположения о нормальности это неверно.

16*. Определим на *множестве смежных классов* группы G по нормальной подгруппе H *операцию умножения* равенством: $gH * fH = g \cdot fH$. Проверить, что это определение корректно, т. е. если $g_1H = gH$, $f_1H = fH$, то $gH * fH = g_1H * f_1H$, и что рассматриваемое множество превращается в группу, обозначаемую далее G/H и называемую *факторгруппой* группы G по подгруппе H .

Докажите, что отображение φ из G в G/H , определяемое равенством $\varphi(g) = gH$, является *гомоморфизмом* групп, т. е. переводит произведение в произведение.

17*. Докажите, что $\mathbb{Z}/m\mathbb{Z}$ изоморфна $\mathbb{Z}_m$.

18*. Найдите факторгруппу группы перестановок n -элементного множества по подгруппе четных перестановок.

§ 2.5. Кольца и поля вычетов

Напомним обозначение: $a \equiv b \pmod{m}$ тогда и только тогда, когда $m \mid a - b$ (читается « a сравнимо с b по модулю m »).

В упражнении 5 из § 2.4 установлено, что сравнения можно почленно складывать и умножать. Это дает возможность на множестве

$$\mathbb{Z}/m\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{m-1}\}$$

всех смежных классов по подгруппе $m\mathbb{Z}$ (через a обозначается смежный класс, содержащий a , т. е. множество $\{a + mn: n \in \mathbb{Z}\}$) определить следующим образом операции сложения и умножения:

$$\bar{a} + \bar{b} = \overline{a + b}, \quad \bar{a} \cdot \bar{b} = \overline{a \cdot b}.$$

Таблицы этих операций состоят из равенств

$$\bar{k} + \bar{l} = \begin{cases} \overline{k + l}, & \text{если } k + l < m, \\ \overline{k + l - m}, & \text{если } k + l \geq m, \end{cases}$$

$$\bar{k} \cdot \bar{l} = \begin{cases} \overline{k \cdot l}, & \text{если } k \cdot l < m, \\ \overline{k \cdot l - m \cdot q}, & \text{если } m \cdot q \leq k \cdot l < m \cdot (q + 1). \end{cases}$$

Если обозначить через r_a остаток от деления a на m , то эти равенства записываются в виде:

$$\bar{r}_{a+b} = \bar{r}_a + \bar{r}_b = \bar{a} + \bar{b}, \quad \bar{a} \cdot \bar{b} = \bar{r}_a \cdot \bar{r}_b = \bar{r}_{a \cdot b}.$$

Множество $\mathbb{Z}/m\mathbb{Z}$ относительно сложения является изоморфной группе $(\mathbb{Z}_m, +)$ коммутативной группой. Относительно умножения оно является коммутативной полугруппой, нейтральным элементом которой является $\bar{1}$.

Упражнение 38. Докажите сформулированные утверждения, а также следующее тождество (*дистрибутивность*): $(x + y)z = xz + yz$.

Определение 49. Множество $(\mathbb{Z}_m, +, \cdot)$ с введенными операциями сложения и умножения называется *кольцом вычетов по модулю m* .

Определение 50. Вообще *кольцом* называется любое множество K с двумя двуместными операциями « $+$ » (сложение) и « $\cdot$ » (умножение), если эти операции связаны *дистрибутивным тождеством*, $(K, +)$ является *коммутативной группой*, а $(K, \cdot)$ — *коммутативной полугруппой*.

Например, $(\mathbb{Z}_m, +, \cdot)$ является кольцом.

Нейтральный элемент относительно сложения обозначается 0, а нейтральный элемент относительно умножения обозначается 1.

Упражнение 39. Совпадение 0 и 1 возможно лишь в кольце, состоящем из одного элемента. В любом кольце выполняются тождества:

$$0 \cdot x = 0, \quad 1 \cdot x = x, \quad (-1) \cdot x = -x.$$

Определение 51. Отображение $\varphi: K \rightarrow \tilde{K}$ является *гомоморфизмом* колец, если $\varphi(1) = \tilde{1}$, для любых $x, y \in K$

$$\varphi(xy) = \varphi(x) \otimes \varphi(y), \quad \varphi(x + y) = \varphi(x) \oplus \varphi(y),$$

где « $+$ » и « $\cdot$ » — операции в кольце K , а « $\otimes$ » и « $\oplus$ » — в кольце $\tilde{K}$. Взаимно однозначный гомоморфизм называется *изоморфизмом*.

Лемма 9. Если φ — гомоморфизм $K \rightarrow \tilde{K}$, то

$$\varphi(0) = 0, \quad \varphi(-x) = -\varphi(x).$$

Доказательство. Пусть $a \in K$, тогда

$$\varphi(a) = \varphi(0 + a) = \varphi(0) + \varphi(a) \Rightarrow \varphi(0) = \tilde{0},$$

$$\varphi(a - a) = \varphi(a) + \varphi(-a) = \tilde{0} = \varphi(0) \Rightarrow \varphi(-a) = -\varphi(a). \quad \square$$

Заметим, что отображение $\varphi: \mathbb{Z} \rightarrow \mathbb{Z}_m$, задаваемое равенством $\varphi(x) = x \pmod{m}$, является гомоморфизмом колец.

Введем несколько определений.

Определение 52. Элемент $a \in K$ называется *обратимым*, если найдется $b \in K$ такой, что $a \cdot b = 1$. Множество всех обратимых элементов кольца K обозначим K^* .

Заметим, что если $ab = 1 = ac$, то $b = c$. Действительно, умножив равенство $ab = ac$ на b , имеем $bab = bac \Rightarrow 1 \cdot b = 1 \cdot c \Rightarrow b = c$. Это позволяет ввести для элемента, обратного к a (относительно умножения), обозначение a^{-1} , так как обратный элемент, если он есть, определен однозначно.

Определение 53. Элемент $a \in K$ называется *делителем нуля*, если найдется $b \in K \setminus \{0\}$, для которого $a \cdot b = 0$. Множество всех делителей нуля K обозначим K^0 .

Имеет место

Теорема 36 (о делителях нуля и обратимых элементах). *Справедливы следующие утверждения: $(K^*, \cdot)$ — группа, $(K \setminus K^*, \cdot)$ и $(K^0, \cdot)$ — полугруппы без единицы, причем K^0 содержится в $K \setminus K^*$, $(K \setminus K^0, \cdot)$ — полугруппа, причем K^* содержится в $K \setminus K^0$. Все упомянутые группы и полугруппы коммутативны.*

Доказательство. Согласно определениям K^* и K^0 справедливы следующие утверждения:

$$1 \in K^*, \quad a \in K^* \Rightarrow a^{-1} \in K^*, \quad K^* \cdot K^* \subseteq K^*$$

(так как $1^{-1} = 1$, $(a^{-1})^{-1} = a$, $(ab)^{-1} = a^{-1}b^{-1}$),

$$K^0 \cap K^* = \emptyset$$

(если $ab = 0$, $a \in K^*$, то $b = b \cdot 1 = (a^{-1}a)b = a^{-1}(ab) = a^{-1}0 = 0$),

$$K^0 \cdot K = K \cdot K^0 \subseteq K^0$$

(если $ab = 0$, $b \neq 0$, то $(a \cdot c) \cdot b = (c \cdot a) \cdot b = c \cdot (a \cdot b) = c \cdot 0 = 0$ при любом $c \in K$),

$$(K \setminus K^0)(K \setminus K^0) \subseteq K \setminus K^0$$

(если $(a \cdot b) \cdot c = 0$, $c \neq 0$, то $(a \cdot b) \cdot c = a \cdot (b \cdot c) = 0$ и поэтому либо $b \in K^0$, либо $bc \neq 0$ и, значит, $a \in K^0$). Выполнение аксиом группы и полугруппы следует из выполнения аксиом ассоциативности, коммутативности и существования единицы в кольце K . $\square$

Из доказанной теоремы вытекают несколько следствий.

Упражнение 40. Докажите, что

$$K^0 \cdot K = K^0, \quad (K \setminus K^0)(K \setminus K^0) = K \setminus K^0, \quad K \cdot (K \setminus K^*) = K \setminus K^*.$$

Следствие 1 из теоремы 36. *Если множество $K \setminus K^0$ конечно (и в частности, если кольцо K — конечно), то $(K \setminus K^0, \cdot)$ — группа и $K \setminus K^0 = K^*$.*

Доказательство. Если $a \in K \setminus K^0$ и $ab = ac$, то $b = c$ (иначе $a(b-c) = 0$, $b-c \neq 0$ и $a \in K^0$). Пользуясь этим и повторяя рассуждения, доказывающие теорему 30, получаем, что для любого $a \in K \setminus K^0$ при некотором $n > 0$, $a^n = 1$, значит, $a^{-1} = a^{n-1} \in K \setminus K^0$, $1 \in K \setminus K^0$, и согласно теоремам 30, 36 видим, что $(K \setminus K^0, \cdot)$ — группа и $K \setminus K^0 = K^*$. $\square$

Упражнение 41. Докажите, что

$$\mathbb{Z}^* = \{1, -1\} \neq \mathbb{Z} \setminus \mathbb{Z}^0 = \mathbb{Z} \setminus \{0\}.$$

Дадим важное

Определение 54. Кольцо K , в котором $K^0 = \{0\}$, называется *целостным*, или *кольцом без делителей нуля*. Кольцо, в котором $K^* = K \setminus \{0\}$, называется *полем*.

Упражнение 42. Целостное кольцо — это такое кольцо, в котором произведение ненулевых элементов всегда отлично от нуля.

Упражнение 43. Поле — это такое кольцо, в котором любой ненулевой элемент всегда имеет обратный элемент относительно умножения, и, значит, всегда возможно деление на ненулевой элемент.

Упражнение 44. Проверить, что $\mathbb{Z}$ — целостное кольцо, но не поле, а $\mathbb{Q}$, $\mathbb{R}$ — поля (и целостные кольца).

Следствие 2 из теоремы 36. *Поле является целостным кольцом. Конечное целостное кольцо является полем.*

Следствие 3 из теоремы 36. *Справедливы равенства*

$$\mathbb{Z}_m^* = \{\bar{a} : (a, m) = 1\}, \quad \mathbb{Z}_m^0 = \mathbb{Z}_m \setminus \mathbb{Z}_m^*.$$

Доказательство. Непосредственно проверяется, что согласно теореме 31

$$\bar{a} \in \mathbb{Z}_m^* \Leftrightarrow \begin{cases} \bar{a} \cdot \bar{x} = \bar{1}, \\ \bar{x} \in \mathbb{Z}_m \end{cases} \Leftrightarrow \begin{cases} x\bar{a} = 1, \\ x \in \mathbb{N} \end{cases} \Leftrightarrow [a] = (\mathbb{Z}_m, +) \Leftrightarrow (a, m) = 1. \quad \square$$

Следствие 4 из теоремы 36. *Кольцо вычетов $\mathbb{Z}_m$ является полем тогда и только тогда, когда p — простое число.*

Теорема 37 (Эйлер). *Если $(a, m) = 1$, $m > 1$, то m делит $a^{\varphi(m)} - 1$, где $\varphi(m)$ — функция Эйлера.*

Доказательство. Так как $(a, m) = 1$ тогда и только тогда, когда $\bar{a} \in \mathbb{Z}_m^*$, а m делит $a^{\varphi(m)} - 1$ тогда и только тогда, когда $\bar{a}^{\varphi(m)} = 1$, то теорему можно сформулировать так: порядок группы $\mathbb{Z}_m^*$ является ее периодом. Но это доказано в теореме 34. $\square$

Следствие из теоремы 37 (малая теорема Ферма). *Если p — простое число, то при любом a число $a^p - a$ делится на p .*

Доказательство. Если p делит a , то это очевидно. Если p не делит a , то $a \in \mathbb{Z}_m^*$ и согласно теореме 37 p делит $a^{\varphi(m)} - 1 = a^{p-1} - 1$, значит, p делит $a^p - a$. $\square$

Теорема 38 (обобщение теоремы Вильсона). *Если F — конечное поле, то произведение всех его ненулевых элементов равно минус единице.*

Доказательство. Так как $x^2 - 1 = (x - 1)(x + 1)$ и в полях нет делителей нуля, то уравнение $x^2 = 1$ в поле имеет ровно 2 решения: $x = 1$ и $x = -1$.

Разобьем все элементы поля F (не равные нулю) на пары взаимно обратных элементов. Так как эти пары попарно не пересекаются, то произведение всех ненулевых элементов поля F равно

$$1 \cdot (-1) \cdot (a_1 \cdot a_1^{-1}) \dots (a_s \cdot a_s^{-1}) = -1. \quad \square$$

Следствие из теоремы 38 (Вильсон). *Число p делит $(p - 1)! + 1$ тогда и только тогда, когда p — простое.*

Доказательство. Если p — простое число, то согласно теореме 38, примененной к полю $\mathbb{Z}_p$, имеем $\bar{1} \cdot \bar{2} \cdot \dots \cdot \overline{p-1} = -1$, откуда $\overline{(p-1)! + 1} = 0$, т. е. p делит $(p - 1)! + 1$.

Если p — составное число, например, $p = m \cdot n$, $m, n > 1$, то p делит $(p - 1)!$, значит, p не делит $(p - 1)! + 1$. $\square$

Задачи и упражнения к § 2.5

1. Если кольцо целостное, то в нем справедлив закон сокращения: $ab = ac$, $a \neq 0 \Rightarrow b = c$. Верно и обратное.

2. Если p — простое, то при любом a число p делит $a^p + (p - 1)!a$ и p делит $(p - 1)!a^p + a$ (это обобщение теорем Ферма и Вильсона одновременно).

3. Докажите, что при целом a число

а) $a^5 - a$ делится на 30;

б) $a^{11} - a$ делится на 66;

в) $a^{17} - a$ делится на 510;

г) $a^{73} - a$ делится на $2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 19 \cdot 37 \cdot 73$.

4*. Найдите какие-нибудь целые a, b такие, что $ab(a + b)$ не кратно 7, а $(a + b)^7 - a^7 - b^7$ делится на 7^7 .

5. Докажите, что если a и m взаимно просты, то найдется единственное b такое, что $0 \leq b < m$ и $ba \bmod m = 1$.

Это число иногда обозначают $a^{-1} \bmod m$.

6. Докажите, что если a и m взаимно просты, то для любого b найдется единственное c такое, что $0 \leq c < m$ и $ca \bmod m = b$.

Это число иногда обозначают $\frac{b}{a} \bmod m$.

7. Если $(a, m) = 1$, то

$$\frac{b}{a} \bmod m = b \cdot a^{\varphi(m)-1} \bmod m.$$

8. Докажите, что определенные выше *символические дроби по модулю m* обладают свойствами обыкновенных дробей:

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}, \quad \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd},$$

и кроме того, если $a \bmod m = c \bmod m$, $b \bmod m = d \bmod m$, то $\frac{a}{b} \bmod m = \frac{c}{d} \bmod m$, если первая из дробей определена.

9. Найдите наиболее простой способ вычисления дробей

$$\frac{a}{2^k} \bmod m, \quad (a, 2) = (m, 2) = 1,$$

и

$$\frac{a}{3^k} \bmod m, \quad (a, 3) = (m, 3) = 1.$$

10*. Докажите для простого p и $0 < b < p$ равенство

$$\frac{a}{b} \bmod p = a(-1)^{b-1} \frac{(p-1) \dots (p-b+1)}{b!} \bmod p.$$

11*. Докажите, что n делит $\varphi(a^n - 1)$ при любом натуральном a .

12. Сравните дроби

$$\frac{116690151}{427863887} \quad \text{и} \quad \frac{3}{11}.$$

13. Правильная обыкновенная дробь $\frac{m}{n}$ представляется конечной десятичной дробью, если и только если n не делится на простые числа, отличные от 2 и 5. Правильная обыкновенная несократимая дробь $\frac{m}{n}$ представляется десятичной дробью с периодом t и предпериодом k , если и только если $10^k(10^t - 1)$ делится на n , причем k и t — наименьшие натуральные числа, удовлетворяющие этому условию. Дробь имеет чисто периодическое разложение, если и только если n не делится ни на 2, ни на 5.

14. Сумма периода и предпериода десятичного разложения любой правильной дроби со знаменателем n не превосходит $\varphi(n)$. Равенство возможно лишь для дробей с чисто периодическим разложением.

15. Длина периода является делителем числа $\varphi(n)$, где n — знаменатель соответствующей обыкновенной дроби. Длина периода равна $\varphi(n)$ для бесконечно многих дробей, например, $1/7^k$, $1/17^k$.

16. Длина периода десятичной записи дроби со знаменателем n не превосходит $n - 1$. Равенство возможно лишь при простом n . При-
мерами таких n служат 7, 17, 29 и даже 1913, однако неизвестно, конечно или бесконечно их количество. К. Ф. Гаусс предположил, что оно бесконечно.

17. Как преобразовать десятичную периодическую дробь в обыкновенную?

18. Сумма или разность двух дробей имеет предпериод, не больший максимума их предпериодов, и период, не больший НОК их периодов.

19. Дроби $1/10^{k_i}(10^{t_i} - 1) = 0,0 \dots 0(0 \dots 01)$, $i = 1, 2$, имеют предпериоды k_i и периоды t_i , а их сумма и разность имеет предпериод $\max(k_1, k_2)$ и период $[t_1, t_2]$.

20. Пусть $u = qv + r$, $0 \leq r < v$, u, v — натуральные числа, q — целое число. Тогда остаток от деления $10^u - 1$ на $10^v - 1$ равен $10^r - 1$. Отсюда выведите, что $(10^u - 1, 10^v - 1) = 10^{(u,v)} - 1$.

21*. Если две дроби имеют предпериоды k_i и периоды t_i , то их произведение имеет предпериод $k \leq k_1 + k_2$ и период

$$t \leq [t_1, t_2](10^{(t_1, t_2)} - 1).$$

Эти неравенства точные и достигаются на дробях $1/10^{k_i}(10^{t_i} - 1)$, $i = 1, 2$.

Из утверждения задачи 21 следует, в частности, что если периоды дробей взаимно просты, то период их произведения не превосходит удвоенного НОК их периодов, но если периоды имеют большой НОД, то период произведения может их значительно превосходить. Так, при возведении в квадрат дроби с периодом t может получиться период $t(10^t - 1)$ (и не может получиться больший).

Указания к задаче 21. Пусть даны две дроби с предпериодами k_i и периодами t_i . Можно считать, что они имеют знаменатели $10^{k_i}(10^{t_i} - 1)$. Период произведения дробей не превосходит наименьшего натурального t такого, что число $10^t - 1$ делится на число $(10^{t_1} - 1) \cdot (10^{t_2} - 1)$. Из задачи 20 выведите, что $t = t_1 n$, n — натуральное число. Тогда число $1 + 10^{t_1} + \dots + 10^{(n-1)t_1}$ делится на $a = 10^{t_2} - 1$. Пусть $r_1, r_2, r_3, \dots$ — остатки от деления чисел $t_1, 2t_1, 3t_1, \dots$ на число at_2 . Тогда последовательность остатков от деления чисел $10^{t_1}, 10^{2t_1}, 10^{3t_1}, \dots$ на число a есть $10^{r_1}, 10^{r_2}, 10^{r_3}, \dots$. Докажите, что последовательность $r_1, r_2, r_3, \dots$ — периодическая с длиной периода $d = t_2/(t_1, t_2)$, ее период $r_1, r_2, r_3, \dots, r_d$ состоит из всех различных чисел из промежутка от 0 до $t - 1$, делящихся на $b = (t_1, t_2)$, и заканчивается нулем. Отсюда следует, что последовательность остатков от деления чисел $10^{t_1}, 10^{2t_1}, 10^{3t_1}, \dots$ на число a — периодическая с длиной периода $d = t_2/(t_1, t_2)$, ее период $10^{r_1}, 10^{r_2}, \dots, 10^{r_d}$ состоит из переставленных

в каком-то порядке чисел $1, 10^b, 10^{2b}, \dots, 10^{(d-1)b}$ и остаток от деления на a числа $s = 1 + 10^{t_1} + \dots + 10^{(n-1)t_1}$ равен при $n = dm$ остатку от деления на a числа

$$m(1 + 10^b + 10^{2b} + \dots + 10^{(d-1)b}) = m \frac{10^{db} - 1}{10^b - 1} = m \frac{10^{t_2} - 1}{10^b - 1}.$$

Следовательно, при $n = (10^b - 1)d$ число s делится на a , а при меньших натуральных n — нет. Выведите отсюда, что наименьшее натуральное t , при котором число $10^t - 1$ делится на число $(10^{t_1} - 1)(10^{t_2} - 1)$, есть число

$$t_1 n = (10^b - 1)dt_1 = (10^b - 1)t_1 t_2 / (t_1, t_2) = [t_1, t_2](10^{(t_1, t_2)} - 1).$$

Рассмотрите дроби $1/10^{k_i}(10^{t_i} - 1)$, $i = 1, 2$. Предпериод их произведения равен $k_1 + k_2$, а период равен минимальному натуральному t такому, что $10^t - 1$ делится на $10^{(t_1, t_2)} - 1$. Таким числом является

$$t = [t_1, t_2](10^{(t_1, t_2)} - 1).$$

§ 2.6. Прямое произведение

Напомним, что прямым (или декартовым) произведением множеств A_1 и A_2 называется множество $A_1 \times A_2 = \{\langle a_1, a_2 \rangle : a_i \in A_i\}$, состоящее из всех упорядоченных пар элементов из A_1 и A_2 .

Определение 55. *Прямым произведением операций $\Box_i: A_i^2 \rightarrow A_i$, $i = 1, 2$, называется операция $\circ: A^2 \rightarrow A$, где $A = A_1 \times A_2$, которая любой паре элементов $\langle a_1, a_2 \rangle \in A$, $\langle b_1, b_2 \rangle \in A$ сопоставляет элемент*

$$\langle a_1 \Box_1 b_1, a_2 \Box_2 b_2 \rangle \in A.$$

Эта операция обозначается $\Box_1 \times \Box_2$.

Определение 56. *Прямым произведением групп $(G_1, \Box_1)$ и $(G_2, \Box_2)$ называется $(G, \circ)$, где $G = G_1 \times G_2$, $\circ = \Box_1 \times \Box_2$.*

Аналогично определяется *прямое произведение полугрупп* и *прямое произведение колец*. С целью краткости, знаки операций опускают, и, например, прямое произведение полугрупп K_1 и K_2 обозначают просто $K_1 \times K_2$ (а операции в ней обозначают, как обычно, знаками «+» и « $\circ$ »). Прилагательное *прямое* тоже часто опускают (если нет опасности спутать прямое произведение с другим типом произведений).

Теорема 39. *Произведение полугрупп является полугруппой, а произведение групп — группой, причем она будет коммутативной, если сомножители коммутативны. Произведение колец является кольцом.*

Доказательство. Выполнение соответствующей аксиомы для произведения следует из выполнения этой аксиомы для сомножителей, если учесть, что в качестве нейтрального элемента произведения можно взять упорядоченную пару, составленную из нейтральных элементов сомножителей, а в качестве элемента, обратного к элементу $\langle a_1, a_2 \rangle$ — элемент $\langle a_1^{-1}, a_2^{-1} \rangle$, где a_i^{-1} обозначает элемент, обратный к a_i относительно соответствующей операции. $\square$

Упражнение 45. Операция произведения групп (полугрупп, колец) коммутативна в том смысле, что, например, кольца $K_1 \times K_2$ и $K_2 \times K_1$ изоморфны.

Упражнение 46. Операция произведения групп (полугрупп, колец) ассоциативна в том смысле, что, например, группы

$$(G_1 \times G_2) \times G_3 \quad \text{и} \quad (G_1 \times G_2) \times G_3$$

изоморфны.

Указанные утверждения дают возможность рассматривать произведение n сомножителей и обозначать их без всяких скобок, например, $G_1 \times \dots \times G_n$ (но такие произведения можно определить и непосредственно обобщая предыдущие определения).

Упражнение 47. Проверьте, что $\Gamma_1 = G_1 \times e_2$ и $\Gamma_2 = e_1 \times G_2$ — подгруппы в $G_1 \times G_2$, где e_i — единица группы G_i , $i = 1, 2$.

Упражнение 48. Проверьте, что $\Gamma_1 \cap \Gamma_2 = \{e_1, e_2\}$ — единичная подгруппа.

Упражнение 49. Имеет место изоморфизм групп $\Gamma_i \cong G_i$, $i = 1, 2$.

Упражнение 50. Справедливо равенство $\Gamma_1 \cdot \Gamma_2 = G_1 \times G_2$.

Упражнение 51. Если $x_i \in \Gamma_i$, $i = 1, 2$, то $x_1 x_2 = x_2 x_1$.

Теорема 40. *Для любых колец K_i имеет место изоморфизм*

$$(K_1 \times K_2)^* = K_1^* \times K_2^*.$$

Доказательство. Достаточно проверить, что $\langle a_1, a_2 \rangle$ принадлежит $(K_1 \times K_2)^*$ тогда и только тогда, когда a_i принадлежит K_i^* , $i = 1, 2$, и применить теорему 39. $\square$



Упражнение 52. Докажите, что произведение полей не является полем.

Теорема 41. Если $(m, n) = 1$, $m, n > 1$, то имеют место изоморфизм $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$ и изоморфизм $\mathbb{Z}_{mn}^* \simeq \mathbb{Z}_m^* \times \mathbb{Z}_n^*$.

Доказательство. Обозначим $\varphi_k: \mathbb{Z} \rightarrow \mathbb{Z}_k$ гомоморфизм колец, задаваемый равенствами $\varphi_k(a) = \bar{r}_a$, где $\bar{r}_a$ — остаток от деления a на k . Гомоморфизм φ_n естественным образом определяет гомоморфизм колец $\varphi_{m,n}: \mathbb{Z}_{mn} \rightarrow \mathbb{Z}_n$ так, что $\varphi_n = \varphi_{m,n}(\varphi_{mn})$ (проверьте!).

Рассмотрим отображение $\psi: \mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$, задаваемое равенствами $\psi(\bar{a}) = (\varphi_{n,m}(\bar{a}), \varphi_{m,n}(\bar{a}))$. Непосредственно проверяется, что оно является гомоморфизмом колец. Докажем его взаимную однозначность.

Пусть $\psi(\bar{a}) = \psi(\bar{b})$. Тогда $\psi(\bar{e}) = 0$, где $\bar{e} = \bar{a} - \bar{b}$. Если $\psi(\bar{e}) = \bar{0}$, то $\varphi_m, n(\bar{e}) = \bar{0} = \varphi_{n,m}(\bar{e})$, т. е. $e \mid n$ и $e \mid m$. Так как $(m, n) = 1$, то отсюда следует, что $e \mid nm$, т. е. $\bar{e} = \bar{0}$, значит, $\bar{a} = \bar{b}$. Итак, имеет место изоморфизм $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$. Из теоремы 40 следует изоморфизм $\mathbb{Z}_{mn}^* \simeq \mathbb{Z}_m^* \times \mathbb{Z}_n^*$. $\square$

Следствие из теоремы 41 (Эйлер). Для любых взаимно простых m, n справедливо равенство (мультипликативность функции Эйлера)

$$\varphi(mn) = \varphi(m)\varphi(n).$$

Доказательство. Если $m = 1$ или $n = 1$, то формула очевидна. Если $m, n > 1$, то она следует из того, что $|\mathbb{Z}_{mn}^*| = |\mathbb{Z}_m^*| \cdot |\mathbb{Z}_n^*|$. $\square$

Упражнение 53. Докажите, что $\varphi(p^n) = p^n - p^{n-1} = p^{n-1}(p - 1)$ при $n \geq 1$.

Теорема 42 (Эйлер). Если $m = p_1^{\alpha_1} \dots p_n^{\alpha_n}$ — каноническое разложение m на простые множители, то

$$\begin{aligned} \varphi(m) &= \varphi(p_1^{\alpha_1}) \dots \varphi(p_n^{\alpha_n}) = \\ &= p_1^{\alpha_1} \dots p_n^{\alpha_n} \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_n}\right) = m \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_n}\right). \end{aligned}$$

Доказательство. Индукция по n с использованием следствия из теоремы 41 и предыдущего упражнения. $\square$

Теорема 43 (китайская теорема об остатках). Если $m_1, \dots, m_n$ попарно взаимно просты, то система сравнений $x_i \equiv r_i \pmod{m_i}$, $i = 1, \dots, n$, равносильна одному сравнению $x \equiv r \pmod{m}$, где $m = m_1 \dots m_n$, а r — некоторое число, $0 \leq r \leq m - 1$.

Доказательство. Индукция по n с использованием теоремы 41. $\square$

Далее до конца параграфа речь пойдет только о коммутативных группах.

Если $H_i \leq G$, то определим сумму множеств H_i равенством

$$H_1 + H_2 = \{h_1 + h_2: h_i \in H_i\}.$$

Докажем несколько теорем, которые понадобятся в следующих параграфах, но представляют также и самостоятельный интерес.

Теорема 44. Если $G = H_1 + H_2$, $H_1 \cap H_2 = \{0\}$, $H_i \leq G$, то

$$G \simeq H_1 \times H_2.$$

Доказательство. Каждый элемент $g \in G$ единственным образом представляется в виде $g = h_1 + h_2$, $h_i \in H_i$, $i = 1, 2$.

Действительно, если $h'_1 + h'_2 = h_1 + h_2$, $h'_i \in H_i$, то $h'_1 - h_1 \in H_1$, $h'_2 - h_2 \in H_2$, а так как $h'_1 - h_1 = h'_2 - h_2$, то

$$h'_1 - h_1 = h'_2 - h_2 \in H_1 \cap H_2 = \{0\},$$

т. е. $h'_1 = h_1$, $h'_2 = h_2$.

Сопоставляя каждому $g \in G$ пару $(h_1, h_2) \in H_1 \times H_2$ такую, что $g = h_1 + h_2$, получаем изоморфизм между G и $H_1 \times H_2$ (проверьте!). $\square$

Если $H \leq G$, m — целое число, то определим mH равенством

$$mH = \{mh : h \in H\} \leq G.$$

Теорема 45 (о разложении группы в произведение). Если $t(G) = mn$, $(m, n) = 1$, то

$$G = mG \times nG, \quad t(mG) = n, \quad t(nG) = m.$$

Доказательство. Так как $t(G) = mn$, то $mnG = \{0\}$, и если $0 < t < mn$, то $tG \neq \{0\}$. Значит, $t(mG) = n$, $t(nG) = m$. Из теоремы 32 следует, что найдутся целые u, v , для которых $tu + nv = 1$. Для любого элемента g из G справедливы равенства

$$g = (tu + nv)g = (tu)g + (nv)g = m(ug) + n(vg) \in mG + nG,$$

т. е. $G = mG + nG$.

Если $g \in mG \cap nG$, то

$$g = (tu)g + (nv)g = u(mg) + v(ng) = u \cdot 0 + v \cdot 0 = 0,$$

так как $g \in nG \cap mG$, $t(nG) = m$, $t(mG) = n$, откуда $mg = 0 = ng$. Остается применить теорему 44. $\square$

Определение 57. Группа G называется p -группой, если ее период — простое число.

Следствие из теоремы 45. Любая конечная коммутативная группа получается из своих p -подгрупп с помощью операции прямого произведения.

Доказательство. Пусть $t(G) = m = q_1 \dots q_n$, $q_i = p_i^{\alpha_i}$, p_i — простые числа, группа $G_i = \frac{m}{q_i} G$ является p_i -подгруппой группы G , $t(G_i) = q_i$, $i = 1, \dots, n$. Применяя индукцию по n и теорему 45, получаем, что

$$G = G_1 \times G_2 \times \dots \times G_n. \quad \square$$

З а м е ч а н и е. Любая конечная p -группа разлагается в прямое произведение циклических p -групп, но мы не будем это доказывать (и использовать).

Теорема 46 (характеристика циклических групп). *Произвольная группа G является конечной циклической, если и только если это коммутативная группа, период которой равен ее порядку.*

Доказательство. Прямое утверждение ($\Rightarrow$) следует из теоремы 31. Докажем обратное утверждение ($\Leftarrow$).

Пусть группа G коммутативна и $t(G) = |G|$. Согласно следствию из теоремы 45 справедливо разложение

$$G = G_1 \times G_2 \times \dots \times G_n,$$

где $t(G_i) = p_i^{\alpha_i}$, p_i — простое, $i = 1, \dots, n$, $t(G) = p_1^{\alpha_1} \dots p_n^{\alpha_n}$. Из условия $|G| = t(G)$ и теоремы 33 следует, что

$$p_1^{\alpha_1} \dots p_n^{\alpha_n} = |G| = |G_1| \dots |G_n| \geq t(G_1) \dots t(G_n) = p_1^{\alpha_1} \dots p_n^{\alpha_n},$$

значит, $|G_i| = t(G_i) = p_i^{\alpha_i}$, $i = 1, \dots, n$. Применяя еще раз теорему 34, получаем, что для некоторого $g_i \in G_i$

$$|g_i| = t(G_i) = |G_i| = p_i^{\alpha_i}, \quad i = 1, \dots, n,$$

значит, $G_i = [g_i]$, т. е. G_i — циклическая группа. Из теоремы 41 с помощью индукции по n получаем, что

$$G = G_1 \times G_2 \times \dots \times G_n$$

— тоже циклическая группа. $\square$

Докажем еще следующую теорему.

Теорема 47 (о периоде произведения групп). *Для любых групп G_1, G_2 справедливо равенство $t(G_1 \times G_2) = \text{НОК}(t(G_1), t(G_2))$.*

Доказательство. Если $t(G_1 \times G_2) = n$, то

$$\{0\} = n(G_1 \times G_2) = nG_1 \times nG_2,$$

откуда $nG_1 = \{0\} = nG_2$, т. е. $t(G_i) \mid n$, $i = 1, \dots, n$, значит, согласно упражнению 1 из § 2.3 $[t(G_1), t(G_2)]$ делит n . В тоже время, если обозначить

$[t(G_1), t(G_2)]$ через m , то

$$m(G_1 \times G_2) = mG_1 \times mG_2 = \{0\} \times \{0\} = \{0\},$$

так как $t(G_i)$ делит m , $i = 1, 2$. Поэтому $m = n$. $\square$

Следствие из теоремы 47. *Изоморфизм $\mathbb{Z}_n \times \mathbb{Z}_m \simeq \mathbb{Z}_{mn}$ имеет место тогда и только тогда, когда $(n, m) = 1$.*

Задачи и упражнения к § 2.6

1. Найдите наименьшее натуральное число, которое при делении на n дает остаток $n - 1$, а при делении на $n + 1$ — остаток n .

2. Число при делении на 2002 дает остаток 2001, а при делении на 2001 — остаток 1901. Какой остаток дает оно при делении на $2002 \cdot 2001$?

3. Найдите четырехзначное натуральное число, которое при делении на 131 дает в остатке 112, а при делении на 132 дает в остатке 98.

4. Окружность разделена n точками на n равных дуг. Сколько различных замкнутых ломаных можно составить из n равных звеньев с вершинами в этих точках (ломаные, получающиеся друг из друга поворотом, считаются одинаковыми)?

5. Докажите, что любую правильную дробь вида $\frac{n}{m_1 \dots m_n}$ можно представить в виде алгебраической суммы (т. е. суммы, в которой могут встречаться слагаемые со знаком минус) правильных дробей вида n_i/m_i , если числа m_i попарно взаимно просты.

6. Найдите сумму всех правильных несократимых дробей со знаменателем n .

7. Докажите, что число всех правильных несократимых дробей со знаменателем n четно.

8. Докажите, что число всех правильных несократимых дробей со знаменателем $a^n - 1$ кратно n .

9. Пусть m_i попарно взаимно просты, $M_i = m_1 \dots m_n/m_i$, $M'_i M_i \equiv 1 \pmod{m_i}$. Докажите, что

$$\begin{cases} x \equiv b_i \pmod{m_i}, \\ i = 1, \dots, n \end{cases} \iff x \equiv x_0 \pmod{m_1 \dots m_n},$$

где $x_0 = b_1 M'_1 M_1 + \dots + b_n M'_n M_n$.

10. Пусть T — число решений сравнения

$$a_n x^n + \dots + a_1 x + a_0 \equiv 0 \pmod{m},$$

$$m = m_1 \dots m_n, \quad (m_i, m_j) = 1 \quad \text{при} \quad i \neq j,$$

а T_i — число решений сравнения

$$a_n x^n + \dots + a_1 x + a_0 \equiv 0 \pmod{m}.$$

Докажите, что $T = T_1 \dots T_n$.

11. Пусть $(m_1, m_2) = d$, а $[m_1, m_2] = \text{НОК}(m_1, m_2) = M$. Докажите, что следующая система разрешима тогда и только тогда, когда d делит $b_2 - b_1$ и

$$\begin{cases} x \equiv b_i \pmod{m_i}, \\ i = 1, 2 \end{cases} \iff x \equiv x_0 \pmod{M}, \text{ где } x_0 \in \mathbb{Z}.$$

12. Докажите, что если система $\begin{cases} x \equiv b_i \pmod{m_i}, \\ i = 1, \dots, n \end{cases}$ разрешима, то $x \equiv x_0 \pmod{[m_1, \dots, m_n]}$, где $x_0 \in \mathbb{Z}$.

13. Генерал-аншеф Раевский хочет построить свои войска для парада в равные квадратные каре. Неизвестное ему и вам число солдат, не превосходящее, однако, 20, находится в лазарете. Докажите, что число солдат у генерал-аншефа может быть таким, что независимо от количества находящихся на момент парада в строю он сможет выполнить свое намерение.

14*. Докажите, что найдется арифметическая прогрессия произвольной конечной длины и с ненулевой разностью, состоящая из натуральных чисел, возведенных в степени ≥ 2 .

15*. Многочлен $F(n)$ с целыми коэффициентами при любом целом n делится на одно из чисел $a_1, \dots, a_m$. Докажите, что для некоторого a_i при любом целом n число $F(n)$ делится на a_i .

В следующих задачах p — простое число.

16. Если $p > 2$, то $C_{p-1}^a \equiv (-1)^a \pmod{p}$.

17*. Если $p > 2$, то $C_n^p \equiv [n/p] \pmod{p}$.

18*. Докажите, что если конечная группа коммутативна и все ее элементы, кроме единичного, имеют одинаковый порядок, равный p , то она изоморфна группе $\mathbb{Z}_p^n$.

19*. Любая группа порядка p^2 коммутативна и изоморфна либо $\mathbb{Z}_p^2$, либо $\mathbb{Z}_{p^2}$.

20*. Любая коммутативная группа порядка $2p$ — циклическая.

21*. Докажите, что конечная коммутативная нециклическая группа содержит подгруппу, изоморфную $\mathbb{Z}_p^2$.

§ 2.7. Конечные поля

Введем следующее определение.

Определение 58. *Характеристикой* целостного кольца K (обозначение $\text{char } K$) называется порядок порожденной его единицей подгруппы группы $(K, +)$. Если он бесконечен, то говорят, что $\text{char } K = 0$. Группа $(K, +)$ обычно называется *аддитивной группой* кольца K .

Справедлива

Лемма 10. *Характеристика кольца K (если она положительна) совпадает с минимальным числом $m > 0$, для которого при $a \neq 0$*

$$\underbrace{a + \dots + a}_m = 0.$$

Указанное число m не зависит от выбора $a \in K$.

Доказательство. Пусть $\text{char } K = m > 0$, тогда по определению $\underbrace{1 + \dots + 1}_m = 0$. Следовательно, для любого $a \neq 0$ справедливо равенство $\underbrace{a + \dots + a}_m = a(\underbrace{1 + \dots + 1}_m) = 0$, а для любого $n < m$ справедливо неравенство $\underbrace{a + \dots + a}_n \neq 0$, ибо $\underbrace{1 + \dots + 1}_n \neq 0$. $\square$

Имеет место также

Лемма 11. *Отображение кольца $\mathbb{Z}_m$ в целостное кольцо K , $\text{char } K = m$, задаваемое правилом*

$$\bar{n} \rightarrow \underbrace{1 + \dots + 1}_n,$$

является изоморфизмом, образ которого совпадает с порожденным единицей подкольцом кольца K .

Доказательство. Достаточно проверить, что при $\bar{n} \in \mathbb{Z}_m \setminus \{0\}$ (т. е. $\bar{n} \neq 0$)

$$\underbrace{1 + \dots + 1}_n \neq 0,$$

откуда следует взаимная однозначность рассматриваемого отображения, ибо при $\bar{n} \neq \bar{m}$ выполнено неравенство

$$\underbrace{1 + \dots + 1}_n \neq \underbrace{1 + \dots + 1}_m,$$

а также равенство

$$\underbrace{(1 + \dots + 1)}_n \underbrace{(1 + \dots + 1)}_e = \underbrace{(1 + \dots + 1)}_n e = \underbrace{1 + \dots + 1}_k,$$

где $0 \leq k < m$, $\bar{n} \cdot \bar{e} = \overline{ne} = \bar{k}$ (другими словами, m делит $ne - k$). $\square$

Теперь легко доказывается

Теорема 48 (о подкольцах). *Кольцо характеристики m содержит подкольцо, изоморфное кольцу вычетов $\mathbb{Z}_m$ (а в случае $m = 0$ — кольцу $\mathbb{Z}$), а именно подкольцо, порожденное единицей. Характеристика целостного кольца либо нуль, либо простое число.*

Доказательство. Первое утверждение следует из леммы 11 в случае $\text{char } K > 0$ и легко доказывается в случае $\text{char } K = 0$.

Второе утверждение докажем от противного.

Если для указанного кольца K его характеристика $\text{char } K > 0$ и составная, т.е. $m = n \cdot l$, $n < m$, $l < m$, то для $a = \underbrace{1 + \dots + 1}_k \neq 0$, $\underbrace{1 + \dots + 1}_l = \underbrace{1 + \dots + 1}_m = 0$, что противоречит лемме 10. $\square$

Докажем следующую интересную теорему*.

Теорема 49 (о порядках конечных полей). *Конечное целостное кольцо является полем, имеет простую характеристику и порядок, равный ее степени.*

Доказательство. Теорема вытекает из следствия теоремы 36, теоремы 48, леммы 10 и следующей леммы. $\square$

Лемма 12. *Конечная абелева группа простого периода p изоморфна декартовой степени циклической группы p -го порядка.*

Доказательство. Выберем в рассматриваемой группе G максимальное число ненулевых элементов a_i , $i = 1, \dots, n$, так, чтобы $a_i \notin G_i = [a_1] + \dots + [a_{i-1}]$. Тогда $G = G_{n+1}$, ибо иначе элемент $a \in G \setminus G_{n+1}$ можно было бы добавить к системе $\{a_i\}$.

Из теоремы 35 следует, что группы $[a_i]$ изоморфны группе $\mathbb{Z}_p$. Из теоремы 30 следует, что $[a_i] \cap G_i = \{0\}$, ведь если бы $0 \neq a \in [a_i] \cap G_i$, то $[a_i] = [a] \subseteq G_i$, чего не может быть. Используя теорему 44 и рассуждая по индукции, получаем, что G_{i+1} изоморфна сумме $[a_i] + G_i \cong [a_1] + \dots + [a_i]$, в частности, $G = G_{n+1} \cong \mathbb{Z}_p^n$. $\square$

* Открытую Эваристом Галуа (Evariste Galois, 1811–1832). Мы не пишем после этой теоремы его имя, так как иначе пришлось бы его писать почти после каждой теоремы этой главы, так как именно он ввел понятия группы и поля и заложил основы теории групп и теории полей. Конечные поля были также открыты им и часто называются полями Галуа.

Для доказательства следующей теоремы понадобится

Лемма 13. Пусть G — любая конечная подгруппа группы K^* . Порядок G не превосходит ее периода.

Доказательство. Пусть $\{a_1, \dots, a_m\} = G$, n — период группы G , $m > n$. Представим для любого $x \in K$ элемент $x^n - 1$ в виде

$$(x - a_1) \dots (x - a_n) + b_1(x - a_1) \dots (x - a_{n-1}) + \dots + b_{n-1}(x - a_1) + b_n,$$

где элементы $b_i \in K$ не зависят от x . Для этого, рассуждая по индукции, подбираем зависящие только от $a_1, \dots, a_n$ элементы b_i так, чтобы при раскрытии скобок в суммах

$$(x - a_1) \dots (x - a_n) + b_1(x - a_1) \dots (x - a_{n-1}) + \dots + b_i(x - a_1) \dots (x - a_{n-i})$$

отсутствовали бы слагаемые вида cx^k при $k \geq n - i$, $k \neq n$.

Так как элемент $a_1 \in G$ имеет период, делящий n , то $a_1^n - 1 = 0$, значит, $b_n = 0$, ибо сумма всех слагаемых обнуляется, кроме, быть может, последнего, а значит, и он равен нулю. Аналогично, подставляя вместо x последовательно $a_2, \dots, a_n$, получаем, что $b_{n-1} = \dots = b_1 = 0$, т. е. при всех $x \in K$

$$x^n - 1 = (x - a_1) \dots (x - a_n).$$

Подставляя вместо x элемент $a_{n+1} \in G$, получаем, что

$$(a_{n+1} - a_1) \dots (a_{n+1} - a_n) = a_{n+1}^n - 1 = 0,$$

а это невозможно в целостном кольце. $\square$

Теперь легко доказывается следующая красивая

Теорема 50 (Гаусс). Конечная подгруппа мультипликативной группы K^* целостного кольца K является циклической. В частности, мультипликативная группа конечного поля — циклическая.

Доказательство. Из теоремы 34 и леммы 13 следует, что порядок группы G равен ее периоду, а из теоремы 46 следует, что группа G — циклическая. $\square$

Образующие элементы этой группы в теории конечных полей принято называть *примитивными элементами*.

Теорема 51 (о числе примитивных элементов). Число примитивных элементов в поле порядка q равно $\varphi(q - 1)$, где φ — функция Эйлера.

Доказательство. Все следует из теорем 31 и 50. $\square$

В теории чисел примитивные элементы поля вычетов $\mathbb{Z}_p$ часто называют *первообразными корнями*.

Упражнение 54. Проверить, что элемент $g \in \mathbb{Z}_p$ является первообразным корнем тогда и только тогда, когда для числа g наименьший показатель степени k , при котором $g^k - 1$ кратно p , равен $p - 1$.

Частным случаем теоремы 51 является

Теорема 52 (о первообразных корнях). Для любого простого p среди чисел $1, \dots, p - 1$ найдется ровно $\varphi(p - 1)$ первообразных корней.

Из доказанных теорем легко следуют также следующие утверждения.

Теорема 53 (малая теорема Ферма для конечных полей). В конечном поле порядка q выполнено тождество Ферма $x^q - x = 0$.

Доказательство. При $x = 0$ все очевидно, а при $x \neq 0$ из теорем 31 и 50 следует, что $x^{q-1} = 1$. $\square$

Частным случаем предыдущего утверждения является

Теорема 54 (малая теорема Ферма). Для любого простого p и любого целого a разность $a^p - a$ делится на p .

Задачи и упражнения к § 2.7

1. Докажите, что все поля из четырех элементов изоморфны друг другу.
- 2*. Пусть K — целостное кольцо характеристики p . Докажите, что отображение $x \rightarrow \sigma(x) = x^p$ является изоморфизмом $K \rightarrow K$, а множество его неподвижных элементов образует подполе, изоморфное полю $\mathbb{Z}_p$. Если K — конечное поле порядка $q = p^n$, то σ^n — тождественный изоморфизм, а множество неподвижных элементов изоморфизма σ^k при $k \mid n$ является подполем порядка p .

3. Докажите, что для любых целых $x_1, \dots, x_n$ имеет место сравнение

$$(x_1 + \dots + x_n)^{p^m} \equiv x_1^{p^m} + \dots + x_n^{p^m} \pmod{p}.$$

Выведите отсюда теорему Ферма, а из нее — теорему Эйлера.

4. Докажите, что при простом $p = 4m + 1$ решениями сравнения

$$x^2 + 1 \equiv 0 \pmod{p}$$

будут $x \equiv \pm(2m)! \pmod{p}$.

- 5*. Докажите, что простых чисел вида $4m + 1$ бесконечно много.

6. При простом $p = 4m + 3$ решите сравнение $x^2 \equiv a \pmod{p}$.

7*. Если p и q — простые, $p > 2$, $p \mid a^q + 1$, то либо $p \mid a + 1$, либо $p = 2qm + 1$, где m — натуральное число.

8*. Пусть $p_1, \dots, p_k$ — все различные простые делители числа $p - 1$. Докажите, что число a будет первообразным корнем по простому модулю p тогда и только тогда, когда $a^{(p-1)/p_i}$ не равно единице по модулю p .

9*. Пусть $p_1, \dots, p_k$ — все различные простые делители числа $p^n - 1$. Докажите, что элемент a конечного поля порядка $q = p^n$ будет примитивным тогда и только тогда, когда $a^{(q-1)/p_i}$ не равно единице поля.

10*. Используя бинарный алгоритм возведения в степень из § 3.6, проверьте, что 10 — первообразный корень по модулю 1913.

11*. В поле порядка 2^n любой трехчлен $x^2 - a$ имеет один двукратный корень.

12. Докажите, что при простом p справедливо сравнение $1^n + 2^n + \dots + (p-1)^n \equiv -1 \pmod{p}$, если $p-1$ делит n , и $1^n + 2^n + \dots + (p-1)^n \equiv 0 \pmod{p}$, если $p-1$ не делит n .

13*. Докажите, что при простом p для любых $x_1, \dots, x_{2p-1} \in \mathbb{Z}_p$ сумма всех C_{2p-1}^p выражений вида $((x_{i_1} + \dots + x_{i_p})^{p-1} - 1)$ равна

$$C_{2p-1}^p \equiv C_{2p-1}^{p-1} \equiv \frac{(2p-1) \dots (p+1)}{(p-1)!} \equiv 1 \pmod{p}.$$

У к а з а н и е. Биномиальный коэффициент C_n^k при $p+k > n \geq p$, $k < p$ делится на p .

14*. (А. А. Суслин.) Докажите, что при простом p для любых $x_1, \dots, x_{2p-1} \in \mathbb{Z}_p$ найдется сумма $x_{i_1} + \dots + x_{i_p}$, равная нулю по модулю p .

У к а з а н и е. Примените предыдущую задачу и малую теорему Ферма.

15*. (Ю. И. Ионин.) Докажите, что среди любых $2n-1$ чисел можно выбрать n чисел, сумма которых делится на n .

У к а з а н и е. Примените предыдущую задачу и индукцию с шагом, основанным на переходе от $A(n)$ и $A(m)$ к $A(nm)$.

16*. Для любого натурального числа n и простого p найдутся целые числа x, y, z такие, что а) $p \mid (x^2 + y^2 - n)$; б) $p \mid (x^3 + y^3 + z^3 - n)$.

§ 2.8. Первообразные корни

Справедлива следующая теорема.

Теорема 55 (Гаусс). (i) Группа $\mathbb{Z}_{p^n}^*$ — циклическая, если $p > 2$, p — простое.

(ii) Группа $\mathbb{Z}_{2p^n}^*$ — тоже циклическая.

(iii) Группа $\mathbb{Z}_{2^n}^*$ — циклическая при $n \leq 2$ и изоморфна группе $\mathbb{Z}_2 \times \mathbb{Z}_{2^{n-2}}$ при $n > 2$, значит, нециклическая.

(iv) Все остальные группы $\mathbb{Z}_m^*$ нециклические.

Доказательство. Докажем (i). В силу теорем 37 и 31 достаточно доказать существование элемента $a \in \mathbb{Z}_{p^n}^*$ порядка $\varphi(p^n)$.

Лемма 14. Если $a \equiv b \pmod{m}$, то $\frac{a^n - b^n}{a - b} \equiv na^{n-1} \equiv nb^{n-1} \pmod{m}$.

Доказательство. Используя известное тождество, получаем, что

$$\frac{a^n - b^n}{a - b} = a^{n-1} + a^{n-2}b + \dots + ab^{n-2} + b^{n-1} \equiv na^{n-1} \equiv nb^{n-1} \pmod{m},$$

ибо $a^{n-k}b^{k-1} \equiv a^{n-1} \equiv b^{n-1} \pmod{m}$ согласно условию леммы и правилу перемножения элементов в $\mathbb{Z}_m$. $\square$

Лемма 15. Если $a \equiv 1 \pmod{m}$, то $\frac{a^n - 1}{a - 1} \equiv n \pmod{m}$ и m делит $\frac{a^n - 1}{a - 1}$ тогда и только тогда, когда m делит n .

Доказательство. Первое утверждение следует из предыдущей леммы, а второе — из первого. $\square$

Лемма 16. Существует целое число g такое, что $g^{p-1} \not\equiv 1 \pmod{p^2}$ и порядок элемента g группы $\mathbb{Z}_p$ равен $p - 1$.

Доказательство. Из теоремы 52 следует, что для некоторого целого числа A порядок элемента $\bar{A} \in \mathbb{Z}_p$ равен $p - 1$. Допустим, что $A^{p-1} \equiv 1 \pmod{p^2}$. Тогда положим $g = A + p$ и выведем из леммы 14, что

$$\frac{g^{p-1} - a^{p-1}}{g - 1} \equiv (p - 1)a^{p-2} \not\equiv 0 \pmod{p},$$

откуда

$$g^{p-1} - a^{p-1} = p \frac{g^{p-1} - a^{p-1}}{g - a} \not\equiv 0 \pmod{p^2},$$

значит,

$$g^{p-1} - 1 \not\equiv a^{p-1} - 1 \equiv 0 \pmod{p^2}. \quad \square$$

Лемма 17. Для числа g из леммы 16 и любого натурального n

$$g^{\varphi(p^n)} \not\equiv 1 \pmod{p^{n+1}}, \quad g^{\varphi(p^n)} \equiv 1 \pmod{p^n}$$

и для любого положительного $m < \varphi(p^n)$

$$g^m \not\equiv 1 \pmod{p^n}.$$

Доказательство. Индукция по n . База ($n = 1$) доказана в лемме 16.

Шаг индукции: $n \Rightarrow (n + 1)$. Пусть $g^m \equiv 1 \pmod{p^{n+1}}$, тогда согласно предположению индукции и теореме 31 (i) число $\varphi(p^n)$ делит m , откуда с помощью леммы 15 выводим, что p делит $\frac{g^m - 1}{g^{\varphi(p^n)} - 1}$ тогда и только тогда, когда p делит $\frac{m}{\varphi(p^n)}$. Последнее возможно тогда и только тогда, когда $\varphi(p^{n+1})$ делит m . Но так как p^n делит $g^{\varphi(p^n)} - 1$ и p^{n+1} не делит $g^{\varphi(p^n)} - 1$ согласно предположению индукции, то p^{n+1} делит $g^m - 1$ тогда и только тогда, когда $\varphi(p^{n+1})$ делит m . Значит, $g^{\varphi(p^{n+1})} \equiv 1 \pmod{p^{n+1}}$, и при любых $0 < m < \varphi(p^{n+1})$ справедливо, что $g^m \not\equiv 1 \pmod{p^{n+1}}$. Осталось проверить, что

$$g^{\varphi(p^{n+1})} \not\equiv 1 \pmod{p^{n+2}}.$$

Для этого достаточно убедиться в справедливости сравнения

$$\frac{g^{\varphi(p^{n+1})} - 1}{g^{\varphi(p^n)} - 1} \equiv p \pmod{p^{n+1}},$$

тогда

$$\frac{g^{\varphi(p^{n+1})} - 1}{g^{\varphi(p^n)} - 1} \not\equiv 0 \pmod{p^2},$$

следовательно,

$$g^{\varphi(p^{n+1})} - 1 = (g^{\varphi(p^n)} - 1) \frac{g^{\varphi(p^{n+1})} - 1}{g^{\varphi(p^n)} - 1} \not\equiv 0 \pmod{p^{n+2}}.$$

Положив $a = g^{\varphi(p^n)}$ и учитывая, что p^n делит $a - 1$, получаем с помощью леммы 15 сравнение

$$\begin{aligned} \frac{g^{\varphi(p^{n+1})} - 1}{g^{\varphi(p^n)} - 1} &= \frac{a^p - 1}{a - 1} = 1 + a + \dots + a^{p-1} = \\ &= p + (a - 1) \left(1 + \frac{a^2 - 1}{a - 1} + \dots + \frac{a^{p-1} - 1}{a - 1} \right) \equiv \\ &\equiv p + (a - 1)(1 + 2 + \dots + p - 1) = \\ &= p + (a - 1) \frac{p(p - 1)}{2} \equiv p \pmod{p^{n+1}}, \end{aligned}$$

ибо $\frac{a^k - 1}{a - 1} \equiv k \pmod{p}$, и тем самым лемма доказана.

В случае $n \geq 2$ требуемое утверждение следует уже из более простого сравнения $\frac{a^p - 1}{a - 1} \equiv p \pmod{p^n}$, сразу вытекающего из леммы 15. $\square$

Докажем теперь теорему. Утверждение (i) следует из леммы 17.

Утверждение (ii) следует из пункта (i) и того факта, что согласно теореме 41 имеет место изоморфизм

$$\mathbb{Z}_{2p^n}^* \simeq \mathbb{Z}_2^* \times \mathbb{Z}_{p^n}^* \simeq \mathbb{Z}_{p^n}^*.$$

Докажем утверждение (iii). Для этого потребуется

Лемма 18. *Справедливо сравнение*

$$5^{2^k} \equiv 1 + 2^{k+2} \pmod{2^{k+3}}.$$

Доказательство. Индукция по k . База ($k=1$): $5 = 1 + 2^2 \pmod{2^3}$. Шаг индукции: $5^{2^{k+1}} = (5^{2^k})^2 = ((1 + 2^{k+2}(2s+1))^2 \equiv 1 + 2^{k+3} \pmod{2^{k+4}})$. $\square$

При $n \leq 2$ утверждение (iii) очевидно. Пусть $n > 2$. Из леммы 18 следует, что элемент $\bar{5} \in \mathbb{Z}_{2^n}^*$ порождает циклическую подгруппу индекса 2, так как

$$\bar{5}^{2^{n-2}} = 1, \quad \bar{5}^{2^{n-3}} = \overline{1 + 2^{n-1}} \neq 1,$$

а $|\mathbb{Z}_{2^n}^*| = \varphi(2^n) = 2^{n-1}$. Но $-\bar{1} \notin [\bar{5}]$ (ведь $5^k \not\equiv -1 \pmod{4}$), поэтому согласно следствию из теоремы 47

$$\mathbb{Z}_{2^n}^* = [5] \cup (-\bar{1}) \cdot [5] = \{1, -1\} \cdot [\bar{5}] \simeq \mathbb{Z}_2 \times \mathbb{Z}_{2^{n-2}} \not\simeq \mathbb{Z}_{2^{n-1}}.$$

Докажем (iv). Разлагая m каноническим образом на простые

$$m = p_1^{\alpha_1} \dots p_n^{\alpha_n}$$

и проводя индукцию по n с помощью теоремы 41, получаем, что

$$\mathbb{Z}_m^* = \mathbb{Z}_{p_1^{\alpha_1}}^* \times \dots \times \mathbb{Z}_{p_n^{\alpha_n}}^*.$$

Из (i) и (iii) с помощью теоремы 47 выводим, что период $t(\mathbb{Z}_{p_i^{\alpha_i}})$ четен, кроме случая $p_1 = 2, \alpha_1 = 1$.

Вычисляя период $t(\mathbb{Z}_m^*)$ с помощью теоремы 47, замечаем, что

$$t(\mathbb{Z}_m^*) \leq |\mathbb{Z}_m^*| \cdot 2^{2-n}$$

и $t(\mathbb{Z}_m^*) = |\mathbb{Z}_m^*|$, лишь когда $n = 1, p_1 > 2$ либо $p_1 = 2, \alpha_1 \leq 2$ или когда $n = 2, p_1 = 2, \alpha_1 = 1$. $\square$

Пусть далее до конца параграфа $m = p^n$ или $m = 2 \cdot p^n, p > 2, p$ — простое и $\alpha \in \mathbb{Z}_m^*$ — первообразный корень (в другой терминологии — порождающий или образующий элемент) группы $\mathbb{Z}_m^*$.

Определение 59. Индексом (или дискретным логарифмом) элемента $x \in \mathbb{Z}_m^*$ по основанию α назовем минимальное неотрицательное n такое, что $\alpha^n = x$, и обозначим его $\text{ind}_\alpha x$ или просто $\text{ind } x$.

Теорема 56 (Эйлер—Гаусс). (i) Для любых $x, y \in \mathbb{Z}_m$ справедливы сравнения

$$\begin{aligned}\text{ind } xy &\equiv \text{ind } x + \text{ind } y \pmod{\varphi(m)}; \\ \text{ind } x/y &\equiv \text{ind } x - \text{ind } y \pmod{\varphi(m)};\end{aligned}$$

(ii) Пусть $1 \leq n \leq \varphi(m)$, $(n, \varphi(m)) = d$. Двучлен $x^n - a \in \mathbb{Z}_m[x]$ имеет в $\mathbb{Z}_m$ ровно d корней, если $d \mid \text{ind } a$, и не имеет корней, если d не делит $\text{ind } a$. Все корни принадлежат $\mathbb{Z}_m^*$ и в случае $a = 1$ образуют циклическую подгруппу порядка d , а в общем случае — смежный класс группы $\mathbb{Z}_m^*$ по этой группе.

(iii) Множество всех $a \in \mathbb{Z}_m^*$, при которых двучлен $x^n - a \in \mathbb{Z}_m[x]$ имеет в $\mathbb{Z}_m$ корни, образует циклическую подгруппу порядка $\varphi(m)/d$ в группе $\mathbb{Z}_m^*$, а именно группу корней двучлена

$$x^{\varphi(m)/d} - 1 \in \mathbb{Z}_m[x].$$

(iv) Порядок (в другой терминологии — период) любого элемента $x \in \mathbb{Z}_m^*$ равен $\varphi(m)/(\varphi(m), \text{ind } x)$. В частности, элемент x будет первообразным корнем в $\mathbb{Z}_m^*$ тогда и только тогда, когда

$$(\text{ind } x, \varphi(m)) = 1.$$

(v) Число всех элементов в $\mathbb{Z}_m^*$, имеющих порядок δ , равно $\varphi(\delta)$. В частности, число первообразных корней в $\mathbb{Z}_m^*$ равно $\varphi(\varphi(m))$.

Доказательство. Докажем утверждение (i). Так как

$$x = \alpha^{\text{ind } x}, \quad y = \alpha^{\text{ind } y},$$

то

$$y^{-1} = \alpha^{-\text{ind } y}, \quad xy = \alpha^s, \quad x/y = \alpha^t,$$

где $s = \text{ind } x + \text{ind } y$, $t = \text{ind } x - \text{ind } y$.

С другой стороны,

$$xy = \alpha^{\text{ind } xy}, \quad x/y = \alpha^{\text{ind } x/y},$$

значит,

$$\alpha^{s - \text{ind } xy} = 1 = \alpha^{t - \text{ind } x/y},$$

поэтому

$$s \equiv \text{ind } xy, \quad t \equiv \text{ind } x/y \pmod{\varphi(m)}.$$

Докажем (ii). Из второго следствия теоремы 36 вытекает, что все корни двучлена $x^n - a \in \mathbb{Z}_m[x]$ при $a \in \mathbb{Z}_m^*$ лежат в $\mathbb{Z}_m^*$.

Из теорем 52 и 31 (i), (v) следует, что

$$d \mid \text{ind } a \Leftrightarrow \{x : x \in \mathbb{Z}_m^*, x^n = a\} \neq \emptyset,$$

и все такие элементы a образуют циклическую подгруппу порядка $\varphi(m)/d$. Если $x^n = a = y^n$, то $(x/y)^n = 1$, и обратно, если $y^n = a$, $(x/y)^n = 1$, то $x^n = a$; кроме того, если $x^n = 1$, $y^n = 1$, то $(xy)^n = 1$.

Поэтому из теоремы 30 вытекает, что

$$\{x \in \mathbb{Z}_m^* : x^n = 1\}$$

является подгруппой, а

$$\{x : x^n = a\} \neq \emptyset$$

— смежным классом группы $\mathbb{Z}_m^*$ по этой подгруппе. Из теорем 33, 31, 52 следует, что ее порядок делит $\varphi(m)$ и n , т. е. делит $d = (\varphi(m), n)$, а так как период подгруппы порядка d группы $\mathbb{Z}_m^*$ равен d и $d \mid n$, то множество

$$\{x : x^n = 1\}$$

совпадает с ней и является тем самым циклической подгруппой порядка d .

Докажем (iii). Если $x^n = a$, то согласно теореме 37

$$a^{\varphi(m)/d} = (x^{\varphi(m)})^{n/d} = 1,$$

значит, каждое a , для которого $x^n = a$, принадлежит множеству

$$\{x : x^{\varphi(m)/d} = 1\},$$

и поэтому утверждение (iii) следует из (ii) и уже доказанных утверждений.

Утверждения (iv) и (v) следуют из теорем 55 и 31 (iii), (iv). $\square$

Определение 60. Некратное p целое число называется *вычетом n -й степени* (при $n = 2$ — *квадратичным вычетом*) по модулю p , если сравнение $x^n \equiv a \pmod{p}$ разрешимо.

Определение 61. Символ Лежандра $\left(\frac{a}{p}\right)$ равен 1, если a — квадратичный вычет, и $\left(\frac{a}{p}\right) = -1$, если a — невычет, а также $\left(\frac{a}{p}\right) = 0$, если $a \equiv 0 \pmod{p}$.

Следствие из теоремы 56 (критерий Эйлера). Справедливо сравнение

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

В группе $\mathbb{Z}_p^*$, где $p > 2$, поровну вычетов и невычетов.

Задачи и упражнения к § 2.8

1. Найдите необходимое и достаточное условие того, что арифметическая прогрессия $an + b$ содержит бесконечно много квадратов натуральных чисел.

2. Докажите, что

$$\left(\frac{-1}{p}\right) = \begin{cases} -1, & \text{если } p = 4k + 3; \\ 1, & \text{если } p = 4k + 1. \end{cases}$$

Далее p — простое, $p > 2$.

3. Докажите индукцией, что $(1 + p)^{p^k} \equiv 1 + p^k \pmod{p^{k+1}}$.

4*. Докажите, что элемент $\frac{1+p}{1+p} \in \mathbb{Z}_{p^n}^*$ порождает циклическую подгруппу порядка p^{n-1} , состоящую из всех элементов вида $\frac{1+ps}{1+p}$, $s = 0, 1, \dots, p^{n-1} - 1$.

5*. Докажите, что если натуральное g таково, что $\bar{g}$ — первообразный корень группы $\mathbb{Z}_p^*$, то элемент gp^{n-1} группы $\mathbb{Z}_{p^n}^*$ порождает циклическую подгруппу порядка $p - 1$.

6*. Докажите, что если порядки элементов g и h взаимно просты, то порядок элемента gh равен их произведению.

7*. Используя задачи 4, 5, 6, дайте еще одно доказательство существования первообразного корня в группе $\mathbb{Z}_{p^n}^*$.

8. Докажите, что $\bar{2}$ — первообразный корень в группах $\mathbb{Z}_{5^n}^*$ и $\mathbb{Z}_{3^n}^*$.

9. Докажите, что элемент $\bar{3}$, так же, как и $\bar{5}$, порождает в группе $\mathbb{Z}_{2^n}^*$ циклическую подгруппу порядка 2^{n-2} .

10. Докажите, что если число $\frac{2^n - 2}{n}$ целое, то и число $\frac{2^{2^n-1} - 2}{2^n - 1}$ тоже целое.

11*. Докажите, что для любого нечетного a и $l \geq 1$ число $\frac{a^{2^{l-1}} - 1}{2^l}$ целое.

12*. Найдите наибольшее k , при котором

а) число $(3^{2^n} - 1)/2^k$ — целое,

б) число $(2^{3^n} + 1)/3^k$ — целое.

13. Докажите, что $3^{k+1} \mid (4^m - 4^n)$ тогда и только тогда, когда $3^k \mid (m - n)$.

14. Числа a, b, n — натуральные, n — нечетное, $a^n + b^n$ и $a + b$ делятся на n . Докажите, что

$$\frac{a^n + b^n}{a + b}$$

также делится на n .

15*. Числа $a, b, a \neq b, n$ — натуральные, $a^n - b^n$ делится на n . Докажите, что

$$\frac{a^n - b^n}{a - b}$$

также делится на n .

16*. Если для некоторого целого a

$$a^{n-1} \not\equiv 0, 1 \pmod{n},$$

то число n — составное.

17*. Решите сравнение $x^2 \equiv 1 \pmod{m}$ при произвольном натуральном m .

18. Докажите, что при $(2a, m) = 1$ сравнение $ax^2 + bx + c \equiv 0 \pmod{m}$ равносильно некоторому сравнению $x^2 \equiv q \pmod{m}$.

19*. Докажите, что при простом p сравнение

$$a_n x^n + \dots + a_1 x + a_0 \equiv 0 \pmod{p}$$

равносильно некоторому сравнению

$$b_{p-1} x^{p-1} + \dots + b_1 x + b_0 \equiv 0 \pmod{p}.$$

20*. (Лагранж.) Докажите, что при простом p сравнение

$$a_n x^n + \dots + a_1 x + a_0 \equiv 0 \pmod{p}$$

имеет не более $\max(n, p)$ решений.

21*. Если для любого простого $p, p \mid n - 1$, найдется такое целое число a_p , что $a_p^{(n-1)/p} \not\equiv 1 \pmod{n}$, $a_p^{n-1} \equiv 1 \pmod{n}$, то число n — простое.

22*. Сравнение $x^2 \equiv a \pmod{p^\alpha}$, $p > 2$ — простое, $(a, p) = 1$, имеет два решения, если $\left(\frac{a}{p}\right) = 1$, и не имеет решений, если $\left(\frac{a}{p}\right) = -1$.

23*. Сравнение $x^2 \equiv a \pmod{2^\alpha}$ имеет решение при любом a , если $\alpha = 1$, при $a \equiv 1 \pmod{4}$, если $\alpha = 2$, при $a \equiv 1 \pmod{8}$, если $\alpha > 2$. В остальных случаях оно не имеет решений. Если $x \equiv x_\alpha \pmod{2^\alpha}$ — одно из его решений, то все остальные его решения при $\alpha > 2$ имеют вид

$$\begin{cases} x \equiv -x_\alpha & \pmod{2^\alpha}, \\ x \equiv x_\alpha + 2^{\alpha-1} & \pmod{2^\alpha}, \\ x \equiv -x_\alpha + 2^{\alpha-1} & \pmod{2^\alpha}. \end{cases}$$

24*. Пусть $\sqrt{a}$ — обычный квадратный корень, z — решение сравнения $z^2 \equiv a \pmod{p}$, где $p > 2$ — простое, $(a, p) = 1$,

$$P = \frac{(z + \sqrt{a})^\alpha + (z - \sqrt{a})^\alpha}{2}, \quad Q = \frac{(z + \sqrt{a})^\alpha - (z - \sqrt{a})^\alpha}{2\sqrt{a}}.$$

Докажите, что для любых целых чисел P и Q существует такое целое число Q' , что $QQ' \equiv 1 \pmod{p^\alpha}$, и $x \equiv \pm PQ' \pmod{p^\alpha}$ — решения сравнения

$$x^2 \equiv a \pmod{p^\alpha}.$$

25. Докажите, что среди любых 6 человек найдутся либо трое попарно знакомых, либо трое попарно незнакомых.

26*. (Рамсей.) Семнадцать ученых попарно переписываются по трем темам. Докажите, что среди них найдутся трое, переписывающиеся по одной теме.

У к а з а н и е. Примените предыдущую задачу.

27*. (И. Шур.) Числа от 1 до 16 раскрашены в 3 разных цвета (другими словами, разбиты на 3 непересекающихся непустых подмножества). Докажите, что среди них найдутся числа x , y , z одного цвета такие, что $x + y = z$.

У к а з а н и е. Занумеруем ученых из предыдущей задачи числами от 1 до 17 и пусть каждая пара (i, j) переписывается по теме, связанной с цветом числа $|i - j|$.

28*. В любом конечном поле порядка более 5 найдутся такие ненулевые элементы x , y , z , что $x^2 + y^2 = z^2$.

29.** (А. Диксон.) Для любого простого $p > 13$ найдутся такие некратные p целые числа x , y , z , что $p \mid x^3 + y^3 - z^3$.

У к а з а н и е. Возьмите какой-нибудь первообразный корень g и покрасьте любой ненулевой элемент a поля $\mathbb{Z}_p$ в цвет $i = 0, 1, 2$, если $a = g^{3k+i}$.

Доказательство квадратичного закона взаимности методом Золотарёва*

В этом трудном цикле задач используется введенное в § 1.10 понятие знака перестановки π , который для краткости здесь будем обозначать $\varepsilon(\pi)$. Вначале напомним одну задачу из § 1.10. Знаком перестановки $\pi \in S_n$ называется число $\varepsilon(\pi) = (-1)^{l(\pi)}$, где $l(\pi)$ — число инверсий в π .

1*. Докажите, что $\varepsilon(f \circ g) = \varepsilon(f) \cdot \varepsilon(g)$.

2*. Докажите, что $\varepsilon(\pi) = (-1)^{d(\pi)}$, где $d(\pi)$ — декремент π .

3*. Докажите, что цикл длины k имеет знак $(-1)^{k-1}$.

* Золотарёв Егор Иванович (1847–1878) — выдающийся русский математик, ученик А. Н. Коркина и П. Л. Чебышёва.

4*. Докажите, что

$$\varepsilon(\pi) = \frac{\prod_{i < j} (i - j)}{\prod_{i < j} (\pi(i) - \pi(j))}.$$

5. Докажите, что

$$\varepsilon \begin{pmatrix} 1 & 2 & \dots & n \\ n & n-1 & \dots & 1 \end{pmatrix} = (-1)^{n(n-1)/2}.$$

6. Проверьте, что отображение смены знака $i: \mathbb{Z}_m \rightarrow \mathbb{Z}_m$, задаваемое формулой $x \rightarrow -x \bmod m$, меняет порядок в $\mathbb{Z}_m \setminus \{0\}$ на противоположный и соответствующая перестановка имеет знак $(-1)^{(n-1)(n-2)/2}$.

7. Проверьте, что отображение сдвига $\mathbb{Z}_m \rightarrow \mathbb{Z}_m$, задаваемое формулой $x \rightarrow x + k \bmod m$, является перестановкой и имеет знак $(-1)^{k(n-1)}$.

У к а з а н и е. Примените задачи 1 и 3.

8*. Пусть $I = \mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$, $J = \mathbb{Z}_m = \{0, 1, 2, \dots, m-1\}$. Упорядочим множество $I \times J$ в порядке (называемом *лексикографическим*)

$$\{(0, 0), (0, 1), \dots, (0, m-1), (1, 0), \dots, (1, m-1), \dots, (n-1, 0), \dots, (n-1, m-1)\}.$$

Рассмотрим перестановку, которая переводит этот порядок в порядок

$$\{(0, 0), (1, 0), \dots, (n-1, 0), (0, 1), \dots, (n-1, 1), \dots, (0, m-1), \dots, (n-1, m-1)\}$$

(тоже лексикографический). Докажите, что знак этой перестановки равен

$$(-1)^{\frac{n(n-1)}{2} \frac{m(m-1)}{2}}.$$

9. Пусть далее m, n — взаимно простые нечетные числа. Проверьте, что отображение

$$\pi_{n,m}: \mathbb{Z}_m \rightarrow \mathbb{Z}_m,$$

задаваемое равенством $\pi_{n,m}(x) = nx \bmod m$ (т. е. умножение на n по модулю m), является перестановкой множества $\mathbb{Z}_m$.

Знак перестановки $\pi_{n,m}$ назовем *символом Золотарёва* и обозначим $(n | m)$.

10. Докажите следующие свойства символа Золотарёва:

(i) если $n = n' \bmod m$, то $(n | m) = (n' | m)$,

(ii) $(nn' | m) = (n | m)(n' | m)$.

У к а з а н и е. Примените задачу 1.

11. Докажите, что $(-1 | m) = (-1)^{(m-1)/2}$.

У к а з а н и е. Примените задачу 6.

12*. Докажите, что $(2 | m) = (-1)^{(m^2-1)/8}$.

У к а з а н и е. Примените определение знака перестановки.

13. Докажите, что $(n | p) = n^{(p-1)/2}$ для нечетного простого p .

У к а з а н и е. Примените задачу 4 и заметьте, что вычисление

$$\frac{\prod_{1 \leq i < j < p} (ni - nj)}{\prod_{1 \leq i < j < p} (i - j)} = \prod_{1 \leq i < j < p} n = n^{p(p-1)/2} = n^{(p-1)/2},$$

использующее малую теорему Ферма, можно проделать в конечном поле $\mathbb{Z}_p$.

14. Определим две перестановки σ, τ множества $I \times J$ равенствами

$$\sigma(i, j) = ((mi + j) \bmod n, j), \quad \tau(i, j) = (i, (nj + i) \bmod m),$$

$$0 \leq i < n, \quad 0 \leq j < m.$$

Докажите, что $\varepsilon(\sigma) = (m | n)$, $\varepsilon(\tau) = (n | m)$.

У к а з а н и е. Перестановка σ каждое подмножество вида $I \times \{j\}$ переводит в себя, и на нем действует так же, как перестановка $\sigma_j(i) = mi + j \bmod n$ на множестве I , но последняя согласно задачам 1, 7 и определению $(m | n)$ имеет знак

$$\varepsilon(\sigma_j) = (-1)^{(n-1)j} (m | n) = (m | n),$$

откуда согласно задаче 1

$$\varepsilon(\sigma) = \prod_{j=0}^{m-1} \varepsilon(\sigma_j) = (m | n)^m = (m | n).$$

15. (Закон взаимности в форме Золотарёва.) Докажите, что

$$(m | n)(n | m) = (-1)^{\frac{n(n-1)}{2} \frac{m(m-1)}{2}}.$$

У к а з а н и е. Если обозначить через $\varphi: I \times J = \mathbb{Z}_n \times \mathbb{Z}_m \rightarrow \mathbb{Z}_{nm}$ «китайский» изоморфизм, то $\varphi(\sigma(i, j)) = mi + j$, $\varphi(\tau(i, j)) = nj + i$, поэтому для перестановки $\psi: \mathbb{Z}_{nm} \rightarrow \mathbb{Z}_{nm}$, соответствующей определенной в задаче 8 и меняющей нумерацию $\psi(mi + j) = nj + i$, справедливо равенство $\varphi \circ \tau = \psi \circ \varphi \circ \sigma$, из которого согласно задачам 1, 8 следует равенство

$$\varepsilon(\tau) = \varepsilon(\sigma)(-1)^{\frac{n(n-1)}{2} \frac{m(m-1)}{2}} = \varepsilon(\sigma)(-1)^{\frac{(n-1)}{2} \frac{(m-1)}{2}}.$$

16. Выведите из закона взаимности равенство $(n | m)(n | m') = (n | mm')$. У к а з а н и е. Применить задачу 10.

17*. Пусть $m = p_1 \dots p_k$, где p_i — простые числа, не обязательно различные. Определим *символ Якоби* $\left(\frac{n}{m}\right)$ как произведение символов

Лежандра, определенных в этом параграфе:

$$\left(\frac{n}{m}\right) = \left(\frac{n}{p_1}\right) \dots \left(\frac{n}{p_k}\right).$$

Докажите, что $(n | m) = \left(\frac{n}{m}\right)$, т. е. символы Якоби и Золотарёва совпадают. Тем самым будет доказан и закон взаимности Гаусса в форме Якоби.

У к а з а н и е. Применить задачи 16, 13 и критерий Эйлера из этого параграфа.

Дополнительные задачи и упражнения по теории чисел и теории групп

1. Пусть целые $r_i, s_i, i = 1, \dots, p$, таковы, что

$$\{\bar{r}_i : 1 \leq i \leq p\} = \{\bar{s}_i : 1 \leq i \leq p\} = \mathbb{Z}_p.$$

Докажите, что $\{\bar{r}_i \bar{s}_i : 1 \leq i \leq p\} \neq \mathbb{Z}_p$ при простом $p > 2$.

2. Докажите, что $n \mid (2^n - 1)$ при нечетных n .
3. Докажите, что n не делит $2^n - 1$ при $n > 1$.
4. Докажите, что n не делит $3^n + 1$ при нечетных $n > 1$.
- 5*. Докажите, что для любого m можно указать такое n , что среди последних m цифр десятичной записи числа 2^n будет
 - а) более половины девяток,
 - б) более половины нулей.
- 6*. Докажите, что степень двойки может иметь при любом k на k -м месте от конца десятичной записи любую заданную цифру (кроме младшего разряда, который и является концом записи).
- 7*. Докажите, что степень двойки может иметь при любом $k \geq 3$ в разрядах, начиная с $(k + 1)$ -го до $3k$ включительно, любую комбинацию десятичных цифр.
- 8*. Докажите, что при любом заданном m последовательность $2^n \pmod{10^m}$, $n = 0, 1, 2, \dots$, периодическая с периодом длины $4 \cdot 5^{m-1}$ и предпериодом длины m .

9*. Ненулевые элементы поля $\mathbb{Z}_p$, $p > 2$, разбиты на множества A и B так, что произведение любых элементов A принадлежит A , произведение любых двух элементов B также принадлежит A . Докажите, что A — множество квадратичных вычетов, а B — квадратичных невычетов.

10*. Докажите, что для любого n найдется делящееся на n число, десятичная запись которого содержит n единиц, а остальные — нули.

11*. Докажите, что для любого $n > 1$ существуют натуральные числа m, M такие, что $x^n + y^n \not\equiv M \pmod{m}$.

12*. Докажите, что степень двойки может начинаться с любой комбинации цифр.

13*. Докажите, что

$$(a^n - b^n, n) = \left(\frac{a^n - b^n}{a - b}, n \right),$$

где a, b, n — натуральные числа.

14*. Докажите, что если при натуральных a, n число $(a^n - 1)/(a - 1)$ есть степень простого числа, то n — тоже простое число.

15*. (Д. Загир.) Пусть p — простое число вида $4k + 1$. Докажите, что преобразование

$$f(x, y, z) = \begin{cases} (2y - x, y, x - y + z), & \text{если } y - z < x < 2y; \\ (x - 2y, x - y + z, y), & \text{если } 2y < x; \\ (x + 2z, z, y - x - z) & \text{в остальных случаях} \end{cases}$$

является перестановкой порядка 2 на множестве всех натуральных решений уравнения $x^2 + 4yz = p$, имеющей лишь одну неподвижную точку, именно, $(1, 1, k)$.

16*. (Д. Загир.) Докажите, что уравнение $x^2 + 4yz = p$ имеет нечетное число натуральных решений, и так как преобразование $g(x, y, z) = (x, z, y)$ тоже является перестановкой порядка 2 на множестве всех его натуральных решений, оно имеет хотя бы одну неподвижную точку, т. е. точку вида (x, y, y) , где $x^2 + 4y^2 = p$.

17*. Докажите, что простое вида $4k + 1$ представимо в виде суммы двух квадратов ровно одним способом (с точностью до перестановки слагаемых), а простые вида $4k + 3$ непредставимы таким образом.

18*. Пусть $n = (2^{2p} - 1)/3$, $p > 3$, — простое число. Докажите, что а) $n \mid 2^{2p} - 1$; б) $4p(2^{p-1} + 1) \mid n - 1$; в) $n \mid 2^n - 2$.

19*. (Чебышёв.) Применяя квадратичный закон взаимности, докажите, что 2 — первообразный корень по модулю простого числа p вида $4q + 1$, где q — простое, и по модулю простого числа p вида $2q + 1$, где $q = 4k + 1$ — простое. Если же в последнем случае простое $q = 4k + 3$, то первообразным корнем по модулю $p = 2q + 1$ будет минус два.

20*. (Чебышёв.) Применяя квадратичный закон взаимности, докажите, что 3 есть первообразный корень по модулю простого числа Ферма $2^{2^n} + 1$. Применяя квадратичный закон взаимности, докажите, что 3 есть первообразный корень по модулю простого числа вида $4 \cdot 2^m N + 1$, где $N > 9^{2^m}/(4 \cdot 2^m)$ — также простое.

21. (Чебышёв.) Применяя предыдущие задачи, проверьте, что два будет первообразным корнем по модулям 11, 59, 83, 107, 123; три будет первообразным корнем по модулям 5, 17, 89, 137, 233, 257, 569, 809, 857, 6737, 65537; минус два будет первообразным корнем по модулям 7, 13, 47.

22*. Монотонная функция обладает свойством *мультипликативности*: для любых взаимно простых m и n для ее значений справедливо равенство

$$f(mn) = f(m)f(n).$$

Докажите, что $f(n) = n^\alpha$ для любого натурального числа n .

23. Пусть $a_1, \dots, a_n$ — не обязательно различные элементы группы порядка n . Докажите, что произведение нескольких подряд идущих элементов равно единице.

24. Можно ли группу представить в виде объединения двух собственных подгрупп?

25*. Любая конечная группа более чем из двух элементов имеет нетождественный автоморфизм.

У к а з а н и е. Если группа некоммукативна, то она имеет нетождественный автоморфизм вида $x \rightarrow axa^{-1}$. Если она коммутативна и не каждый квадрат в ней равен единице, то автоморфизм $x \rightarrow x^{-1}$ — нетождественный. В оставшихся случаях она изоморфна группе $(\mathbb{Z}_2)^n$.

26*. (С. В. Конягин.) Пусть n — наименьшее число элементов a_i , $i = 1, \dots, n$, в конечной абелевой группе G , такое, что любой элемент G можно представить в виде $\pm a_{i_1} \pm a_{i_2} \pm \dots$. Докажите, что

$$\log_3 |G| \leq n \leq \log_2 |G|.$$

У к а з а н и е. Для получения верхней оценки выберите максимальное множество элементов a_i , $i = 1, \dots, n$, такое, что все их суммы будут попарно различны.

27.** Докажите, что существует сколь угодно много подряд идущих натуральных чисел, не представимых в виде суммы квадратов двух натуральных чисел.

§ 2.9. Алгебра и криптология

Читатель уже имеет представление, что такое алгебра. А что такое криптология? До недавнего времени это слово можно было услышать только на специальных курсах в некоторых специальных учебных заведениях. Но сейчас оно стало мелькать на страницах научных журналов и в трудах конференций. Был открыто опубликован первый в России учебник по криптографии, написанный преподавателями академии ФСБ. Начала появляться и популярная литература по этому вопросу, в том числе перевод написанной еще в 1970-е годы книги Д. Кана «Взломщики кодов» (М.: Центрполиграф, 2000).

Нам кажется уместным дать здесь краткий, в основном исторический, обзор на эту тему.

Криптология делится на два направления — криптографию и криптоанализ. *Криптография** защищает информацию с помощью *шифрования* открытого текста, на жаргоне криптографов называемого французским словом *клер*.

Определение 62. *Шифрование* — это обратимое преобразование клера в *шифртекст*. Оно определяется двумя взаимно обратными отображениями $E_k: T \rightarrow C$ и $D_k: C \rightarrow T$, где T — множество всех клеров, C — множество всех шифртекстов, k — *ключ*, выбираемый из *пространства ключей* K . Если обозначить через E множество $\{E_k: k \in K\}$ всех отображений шифрования а через D множество $\{D_k: k \in K\}$ всех отображений расшифрования, то для любых $t \in T$, $k \in K$ выполняется равенство $D_k(E_k(t)) = t$. Тогда совокупность (T, C, K, E, D) назовем *шифром*, или *шифр-системой*.

Простейшими и старейшими классами шифров являются шифры перестановки и шифры замены. В этих шифрах $C = T = A^n$, где A — алфавит текста, n — длина сообщения.

Определение 63. Роль ключа k в *шифре перестановки* играет произвольная перестановка $k \in S_n$ из группы перестановок множества $\{1, \dots, n\}$; таким образом, пространство ключей $K = S_n$, отображение шифрования определяется равенством

$$E_k(a_1 a_2 \dots a_n) = a_{k(1)} a_{k(2)} \dots a_{k(n)},$$

а отображение расшифрования определяется равенством

$$D_k(a_1 a_2 \dots a_n) = a_{k^{-1}(1)} a_{k^{-1}(2)} \dots a_{k^{-1}(n)}.$$

Определение 64. Роль ключа k в *шифре замены* играет произвольная перестановка $k \in S_A$ из группы перестановок алфавита A ; таким образом, пространство ключей $K = S_A$, отображение шифрования определяется равенством

$$E_k(a_1 a_2 \dots a_n) = k(a_1) k(a_2) \dots k(a_n),$$

а *отображение расшифрования* определяется равенством

$$D_k(a_1 a_2 \dots a_n) = k^{-1}(a_1) k^{-1}(a_2) \dots k^{-1}(a_n).$$

Уже из этих определений видна связь криптографии с алгеброй. Из следующих далее примеров мы увидим, что старейшими применениями группы перестановок алгебра обязана именно криптографии.

* Тайнопись в переводе с греческого.

Примеры. 1. Первый шифр перестановки, согласно Плутарху, использовали в Спарте. На цилиндр, который назывался *сцитала*, плотно наматывалась узкая пергаментная лента. Вдоль оси цилиндра записывался текст. Лента сматывалась и передавалась адресату, который читал сообщение, наматывая ленту на такую же сциталу. Ключом к шифру является диаметр сциталы. Первый же успешный метод вскрытия шифра приписывается Аристотелю, который предложил наматывать ленту на конус, сдвигая ее от вершины к основанию конуса. Там, где диаметр конического сечения совпадал с диаметром сциталы, на ленте проступали осмысленные слоги и слова, после чего изготовлялась сцитала соответствующего диаметра.

2. Первый шифр замены изобрел Юлий Цезарь. В качестве перестановки букв алфавита использовалась перестановка, которая для современного алфавита выглядит так:

$$\begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z & a & b & c \end{pmatrix}$$

— просто циклический сдвиг на три буквы. Обратная перестановка тоже, естественно, является циклическим сдвигом. В общем случае в этом шифре использовался сдвиг вида $i \rightarrow (i + k) \bmod 26$ и ключом являлось число k . Так как ключевое пространство невелико, алгоритм шифрования Цезарь, видимо, не особо афишировал.

3. Большое ключевое пространство у *аффинного шифра*, так как в нем используются перестановки вида $i \rightarrow (ai + k) \bmod 26$.

4. К классу шифров перестановки относятся шифры *маршрутной перестановки*. Идея у них такая. Сообщение записывается в таблицу по одному маршруту, например по горизонталям, а считывается по другому, например по вертикалям. Для увеличения ключевого пространства использовалась еще перестановка столбцов таблицы.

Кроме указанных двух классов шифров, издавна известны и другие методы шифрования. Например, вторым шифровальным приспособлением в Спарте была *таблица Энея*. На ней горизонтально располагался алфавит, а по боковым сторонам делались выемки для наматывания нити. Нить наматывалась на таблицу, двигаясь по каждой строке в одном направлении, и напротив букв сообщения на ней завязывались узелки, которые и представляли собой шифртекст (фактически в двоичном алфавите). Для чтения сообщения нить наматывалась на ту же таблицу, которая и служила ключом к шифру. История не сохранила сообщений о вскрытии этого шифра.

Древнегреческий историк Полибий описал следующий способ шифрования. Алфавит записывался в квадратную таблицу 5×5 и каждая буква

шифровалась парой своих координат (i, j) (номерами строки и столбца), а передаваться сообщения могли в то время с помощью факелов — i факелов в левой руке и j факелов в правой означали пару (i, j) .

Кстати, этот шифр представляет, вероятно, первый пример так называемого *алфавитного кодирования*, которое заключается в том, что каждая буква алфавита сообщения заменяется на слово в более коротком *шифроалфавите*.

Дальнейшее развитие идеи алфавитного кодирования принадлежит знаменитому английскому философу, эзотерику и писателю сэру Френсису Бэкону, который начал использовать двоичный алфавит в качестве шифроалфавита. В криптографии, правда, это не нашло особого применения, главным образом из-за пятикратного удлинения шифртекста в сравнении с клером, но зато эта идея легла в основу телеграфных кодов (азбука Морзе), которые сейчас вышли из употребления и их роль в каком-то смысле играют компьютерные коды, например, ASCII-код, а также, например, в основу кодов Брайля, на которых пишут книги для слепых, или штрих-кодов на товарных наклейках*.

Возвращаясь к истории, следует сказать, что первые идеи криптографии, такие, как замена символов, появились в Древнем Египте и Шумере. Но использовалась она, вероятно, только для шифрования религиозных текстов, медицинских рецептов и пр. Ее развитие сдерживалось слишком большой сложностью идеографического письма.

Первое применение в политических целях криптографии и *криптоанализа*, т. е. науки о чтении криптограмм при неизвестном шифре или ключе к нему, вероятно, принадлежит древним индусам. Правда, не сохранилось информации, как и какие шифры они умели вскрывать.

С тех пор криптография применялась в основном уже с политическими целями. О том, как это делали греки, уже говорилось. После них, как и в математике, эстафету приняли арабы. Само слово «шифр» арабского происхождения. О тайнописи упоминалось даже в сказках «Тысячи и одной ночи». Первую в истории книгу, посвященную описанию некоторых шифров, написал в 855 г. Абу Бакр Ахмед бен Али ан Набати.

В 1412 г. Шехаб аль Кашканди в своей 14-томной энциклопедии поместил раздел под названием «О сокрытии в буквах тайных сообщений», в котором кроме семи разных шифров впервые появилось описание вскрытия шифров *методом частотного анализа*. Статистику встречаемости букв и биграмм он составил на основе текста Корана.

* Черные и белые промежутки в них соответствуют последовательностям нулей и единиц длины от 1 до 4.

С этого момента начинается свою историю криптоанализ. Кстати, этим методом успешно вскрываются аффинные шифры, описанные выше.

В Европе, после периода застоя в темные века и в раннем средневековье, криптография, как и математика, начала бурно развиваться в Италии. Первый зашифрованный текст, хранящийся в архивах Ватикана, датируется XIV в., а первый простейший шифр — XII в.

В XIV в. секретарь Римского папы Габриэль де Лавинда, помимо шифроалфавита с пустышками (ничего не значащими символами), использовал также список часто встречающихся в переписке слов и имен, которые заменялись *кодовыми словами*. Вообще *кодом* называется замена на другие символы не отдельных символов, как в шифре, а целых слов. Список кодируемых слов и их кодовых эквивалентов назывался *номенклатором*. Так же стали называться гибридные системы, сочетающие в себе свойства и шифра, и кода. Со времен Габриэля де Лавинды именно номенклаторы стали на 450 лет основой шифровального дела в Европе.

В 1401 г. в Мантуанском герцогстве был впервые изобретен первый представитель шифров *многозначной замены*, или *омофонов*.

В 1474 г. появилась книга о тайнописи Чико Симонетти, секретаря Миланского герцога. Это был, вероятно, первый в мире трактат, посвященный криптоанализу. В нем излагались правила вскрытия шифров простой замены и высказывалась идея шифров *пропорциональной замены*, в которых число различных замен для каждой буквы было пропорционально частоте ее встречаемости в открытом тексте.

Выдающимся криптографом проявил себя знаменитый итальянский философ, художник и архитектор Леон Альберти *. В 1466 г. в своем труде о шифрах он описал *шифровальный диск*, который состоял из неподвижного большого и подвижного малого соосных дисков, на которых были написаны символы алфавита, причем на большом диске четыре самые редко используемые буквы были заменены на первые четыре цифры. Этот диск реализовывал шифр простой замены Цезаря, роль ключа играла выбранная буква на подвижном диске. Но после того, как была зашифрована часть текста, ключ по определенному правилу менялся, таким образом, Альберти фактически положил начало *многоалфавитным* шифрам, которые стали впоследствии основным классом шифров, используемых с серьезными целями. Кроме того, он составил большой номенклатор, в котором в качестве кодовых слов использовались числа от 11 до 4444. Если слово из номенклатора встречалось в тексте, оно

* Л. Б. Альберти (Leon Battista Alberti, 1404–1472). Сформулировал законы перспективы.

заменялось соответствующим кодом, а потом шифровалось с помощью диска наравне с другими словами. Таким образом, Альберти изобрел *коды с перешифрованием*, получившие широкое распространение только в конце XIX в. Свой шифр он назвал «шифром, достойным королей».

Следующий шаг в развитии многоалфавитных шифров сделал в XVI в. знаменитый философ и эзотерик аббат Иоганн Тритемий, написавший книгу «Стеганография». В ней впервые появилась квадратная таблица для шифрования. В первой ее строке был написан обычный алфавит, во второй строке он был циклически сдвинут влево на одну букву и т. д. Первая буква шифровалась первым алфавитом, вторая — вторым алфавитом и т. д. Таким образом, шифр Тритемия стал первым примером *периодического шифра*. Он имел преимущество перед шифром Альберти, так как шифроалфавиты в нем менялись постоянно, а не через некоторые промежутки, как у Альберти.

В 1553 г. Джованни Баттиста Белазо предложил использовать для шифрования короткий, легко запоминаемый *ключ*, который он назвал *паролем*. Пароль периодически выписывался над шифруемым текстом и его буквы указывали на тот алфавит, который использовался для шифрования соответствующей буквы текста.

Через 10 лет 28-летний Джованни делла Порта опубликовал книгу «О тайной переписке», в которой усовершенствовал идеи Тритемия и Белазо, а также предложил шифр *простой биграммной замены*. В нем с помощью специальной таблицы заменялись на шифросимволы пары букв открытого текста. Этот шифр стал первым из класса *блочных шифров*, в которых текст разбивается на блоки, которые потом шифруются. Шифры с побуквенным шифрованием называются *поточными*.

Знаменитый математик, изобретатель, врач, астролог, эзотерик и криптограф Джироламо Кардано, имя которого еще встретится далее, предложил использовать в качестве ключа сам открытый текст.

Эту идею развил французский криптограф барон Блез де Виженер, который предложил также в таблице Тритемия перемешивать алфавит в первой строке, и с тех пор ее называют таблицей Виженера. В качестве *самоключа* он предложил использовать сам открытый текст, но с добавленной в его начало секретной ключевой буквой, известной получателю.

Несколько отвлекаясь, заметим, что в средние века криптография связывалась не столько с математикой, сколько с магией. В своей книге Д. Кан по существу называет это обывательским предрассудком и объясняет его происхождение тем, что алхимики и астрологи часто зашифровывали свои тексты, а также удивлением от самой возможности вскрытия

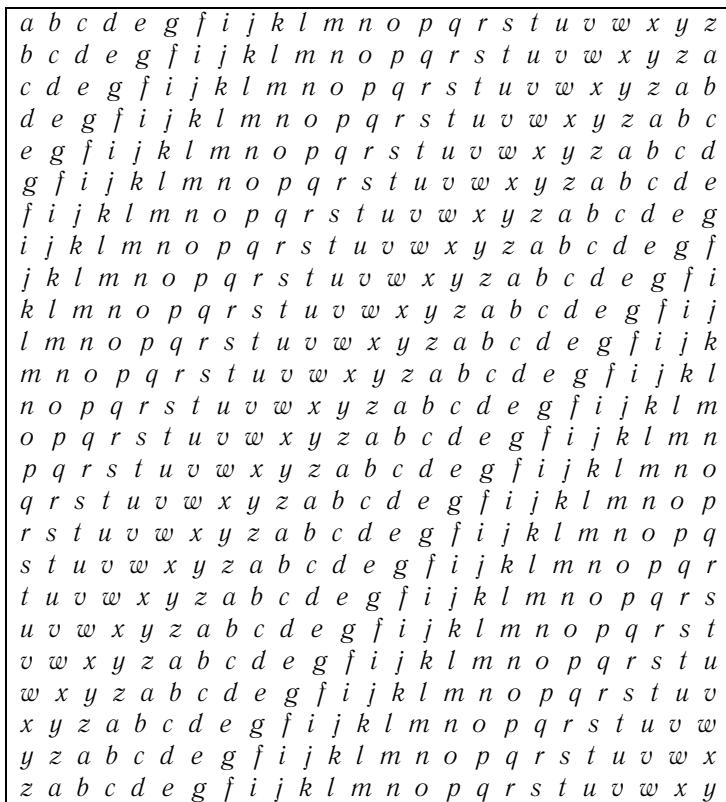


Рис. 20. Квадрат Виженера

шифра. Но этот предрассудок дожил почти до нашего времени, и в написанной в 1928 г. книге американца Мэнли Холла «Энциклопедическое изложение масонской, герметической, каббалистической и розенкрейцевской философии», переведенной у нас в 1992 г., есть раздел о криптографии, написанный отнюдь не с научных позиций. Заметим еще, что так называемая естественная магия, адептами которой были М. Фицино, Пико де Мирандолла, Агриппа, Парацельс, Джордано Бруно и другие, была широко распространена в средневековье. И Тритемий, и Кардано писали о ней в тех же книгах, в которых они описывали свои шифры*.

Кардано также предложил использовать для шифрования *поворотную решетку*. Она представляла собой твердый трафаретный лист, в котором были проделаны прямоугольные прорезы. Лист накладывался

* См. об этом книгу Фр. Йейтс «Джордано Бруно и герметическая традиция».

на бумагу того же размера, а в прорезях писалось сообщение. После снятия решетки на бумаге дописывался текст, маскирующий секретное сообщение.

Подобным методом пользовались, например, кардинал Ришелье и А. С. Грибоедов во время своей дипломатической работы.

Фактически это был метод не столько шифрования, сколько *стеганографии*. Под стеганографией понимаются сейчас методы скрытия самого факта передачи секретного сообщения, чем она отличается от криптографии, в которой сам факт передачи криптограммы никак не маскируется. Как стеганографический метод применял свой двоичный код Френсис Бэкон. Вместо двоичных цифр он использовал обычный алфавит, но со шрифтами двух типов. Таким методом можно было в любом тексте спрятать шифровку, если конечно, шрифты были достаточно мало различимы.

Интересно, что в XIX в., главным образом в кругах, интересующихся наследием возникшего в средневековье тайного мистического ордена розенкрейцеров, появилась идея, что Френсис Бэкон, которого считали розенкрейцером, является настоящим автором пьес Шекспира. Начали искать подтверждение этого в шифрах, которые мог оставить Бэкон в своих книгах, а также в первом знаменитом издании пьес Шекспира. Было, естественно, найдено много таких, якобы зашифрованных, фрагментов. Серьезные исследователи, правда, замечали, что в любом длинном тексте можно при желании и некоторых натяжках найти короткие фрагменты, напоминающие шифры. Но у сторонников авторства Бэкона стремление доказать это криптографическим методом приняло форму мании. Американский миллионер Фабиан даже создал в начале XX в. на свои деньги лабораторию криптоанализа, которая занималась только подобными исследованиями.

Фабиан нанял на работу дипломированного генетика Уильяма Фридмана, сына эмигрантов из России. Через некоторое время Фридман уже возглавлял у Фабиана и лабораторию генетики, имевшую прикладную сельскохозяйственную направленность, и лабораторию криптоанализа. Доказать авторство Бэкона он не смог, более того, он впоследствии опубликовал книгу, где опровергал возможность такого криптографического доказательства. Но он не на шутку увлекся криптографией и своей подчиненной Элизабет Смит, с которой обвенчался в 1917 г. Они стали самой знаменитой супружеской парой в истории криптографии. После вступления Америки в войну у него с супругой появилась серьезная работа по правительственным заказам. После войны он ушел от Фабиана и стал главным криптографом войск связи. Фридман опубликовал выдающиеся работы по криптоанализу, частью у Фабиана, частью позднее, где

изложил свои методы. Сам термин «криптоанализ» был введен Фридрихом. Последним его крупным достижением было вскрытие японского «пурпурного шифра» перед началом Второй мировой войны. Успехи американского криптоанализа сыграли едва ли не решающую роль в победе над Японией.

Переходя к истории криптоанализа, стоит упомянуть среди выдающихся криптоаналитиков секретаря по шифрам Венецианской республики Джованни Соро — первого криптоаналитика, получившего широкую известность в XVI в., выдающегося математика Франсуа Виета, бывшего членом тайного совета Генриха IV, Филиппа ван Марникса, автора мелодии гимна Нидерландов и правой руки Вильгельма Оранского, который во время восстания голландцев и фламандцев против испанского владычества с успехом вскрывал испанские шифры, и первого знаменитого английского криптоаналитика Томаса Фелиппеса, который прочитал зашифрованное письмо Марии Стюарт, находившейся в плену у королевы Елизаветы (и сделал вставку). Эта история закончилась трагически для Марии и показала еще раз, что слабый шифр еще хуже, чем отсутствие шифра вообще.

До XVII в. криптоанализ был формально делом любителей, хотя иногда и выполнявших важные государственные поручения. В XVII в. в Европе появились первые государственные дешифровальные подразделения, называемые неофициально «черными кабинетами». Первый такой кабинет организовал во Франции Ришелье. Начальником кабинета стал первый профессиональный криптограф Франции Антуан Россиньоль, который внес большой вклад в дело совершенствования номенклаторов.

Позднее возник такой кабинет и в Англии. В нем работал крупнейший английский математик того времени Джон Валлис*.

Следующий век не дал новых идей в криптографии, но был временем расцвета черных кабинетов. Во время царствования Петра I они появились и в России. Сам Петр проявлял интерес к криптографии и обсуждал эти проблемы с Лейбницем, которого приглашал в Россию для организации Академии наук. Лейбниц в Россию не поехал, но Академия все равно была создана. Уже после смерти Петра в ней стали работать Эйлер и Даниил Бернулли. При Елизавете с успехом работал черный кабинет, в котором играл важную роль приятель Эйлера, известный математик академик Христиан Гольдбах, получивший за оказанные Российской империи услуги звание тайного советника. Благодаря его деятельности читалась вся дипломатическая переписка.

* Дж. Валлис (John Wallis, 1616–1703) — английский математик и криптограф, один из основателей Лондонского королевского общества.

Эпоха черных кабинетов в основном закончилась в период революционного подъема в XIX в. Но тогда же, в XIX в., возникли новые идеи в криптографии. Появились первые дисковые шифраторы. Один из них был изобретен будущим президентом США Томасом Джефферсоном, но не был применен на практике. Его описание было найдено в его бумагах в 1922 г. Как раз в этом году в армию США стали поступать шифровальные машины, устроенные приблизительно так же. Другие варианты дисковых шифраторов были созданы Д. Уодсвортом в 1817 г. и известным физиком и изобретателем Чарльзом Уитстоном, показавшим свой шифратор в 1876 г. на Всемирной выставке в Париже. Уитстон также изобрел шифр, называемый иногда шифром Плейфера, по имени заместителя председателя палаты общин и его друга, внешне очень на него похожего.

Шифр Плейфера—Уитстона является блочным биграммным шифром простой замены. В квадратную или прямоугольную разбитую на клетки таблицу записаны в перемешанном виде буквы алфавита. Текст разбивается на двубуквенные блоки — биграммы, промежутки между словами заменяются самой редкой буквой алфавита. Произвольная биграмма (a, b) заменяется на биграмму (c, d) которую определяют следующим образом. Находят буквы a, b в таблице Плейфера. Если они не стоят на одной линии (строке или столбце), то берется прямоугольник с вершинами в четырех клетках таблицы, в двух противоположных вершинах которого стоят буквы биграммы (a, b) . Тогда буквы, образующие вторую диагональ, составляют биграмму (c, d) , причем для определенности буква c берется с той же вертикальной линии, что и буква a . Если же буквы a, b стоят на одной линии, то, например, буквы c, d берутся с той же линии, но с циклическим сдвигом на соседнюю клетку по этой линии в фиксированном направлении (вниз или вправо).

В криптоанализе крупного успеха добились независимо друг от друга эксцентричный английский математик и изобретатель Чарльз Бэббидж* и отставной майор прусской пехоты Фридрих Казисски. Им удалось найти метод вскрытия шифра Виженера. Однако Бэббидж не опубликовал своих результатов, возможно, под давлением английского черного кабинета (в это время шла Крымская война), и о них стало известно лишь недавно (опубликовано в книге Саймона Сингха (Singh Simon, Code Book, Doubleday, 1999)). Казисски опубликовал свою книгу в 1863 г., но она не вызвала тогда большого интереса и он перестал заниматься криптографией. Дальнейшее усовершенствование метода Казисски—Бэббиджа опубликовал в своих лекциях по криптоанализу в 1920 г. У. Фридман.

* Ч. Бэббидж (Charles Babbage, 1792—1871).

В XIX в. криптография впервые стала упоминаться и в художественной литературе. Выдающийся американский писатель и поэт Эдгар По, мастер мистической и таинственной новеллы, создатель жанра детектива и литературы ужасов, написал знаменитый рассказ «Золотой жук», в котором описал процесс вскрытия шифра простой замены. Впоследствии вскрытие шифров описывалось также в рассказах о Шерлоке Холмсе А. Конан Дойля. Эдгар По был криптографом-любителем, неоднократно писал о криптографии в журналах, с успехом разгадывал шифровки, присылаемые ему читателями. Он написал также хорошую популярную статью «Криптография», перевод которой опубликован в его двухтомнике, изданном в 1995 г. в Санкт-Петербурге. В частности, в ней изложены некоторые сведения, приведенные нами в этом разделе.

В XX в. криптография развивалась очень бурно. В двадцатые годы были в Голландии Кохом, в Германии Шребиусом, в США Хеберном, а в Швеции Даммом и Хагелиным запатентованы несколько вариантов *колесных шифраторов*. Но только Борису Хагелину, родившемуся в России сыну Цезаря Хагелина, управляющего нефтяной компанией Нобеля, удалось благодаря заказам американской армии добиться коммерческого успеха. Он стал единственным человеком, заработавшим миллионы на криптографии.

Когда компания, основанная Шребиусом, прекратила существование, производящейся ею шифровальной машиной «Энигма» заинтересовались в германской армии и она стала широко использоваться, а ее производство было возобновлено. Работавшему на заводе по ее производству поляку удалось восстановить ее конструкцию, и эта информация дошла до польских криптографов. После начала войны Мариан Режевский, оказавшийся в Англии, указал английским криптографам на возможность вскрытия шифров «Энигмы». В дальнейшей работе участвовал многотысячный коллектив, в котором выдающуюся роль сыграл знаменитый математик Алан Тьюринг. Если бы немецкие шифровальщики пользовались «Энигмой» аккуратно, с соблюдением всех инструкций, то читать их шифровки было бы невозможно. Но разгильдяйство свойственно и немцам...

Информация о том, что англичанам удалось научиться читать шифровки «Энигмы», была рассекречена только в 1970-е годы. Одна из причин была в том, что после войны в Европе она еще использовалась в некоторых странах, причем англичане ее даже продавали.

Успешно развивалась криптография и в США. Во время Первой мировой войны черный кабинет под руководством выдающегося криптоаналитика Ярдли расшифровал тысячи дипломатических телеграмм разных

стран. Но знаменитую телеграмму Циммермана, которая послужила для США одним из формальных поводов объявления войны Германии, прочли англичане (по некоторым версиям, они сумели как-то заполучить немецкие шифры). Однако после войны, вопреки ожиданиям Ярдли, финансирование этой деятельности было прекращено и тогдашний госсекретарь США, впервые узнавший о существовании черного кабинета, произнес легендарную фразу: «Джентльмены не читают писем друг друга». Ярдли оказался без работы и написал книгу о деятельности черного кабинета, а впоследствии роман, по которому был снят фильм. Книга имела скандальный успех и была переведена на несколько языков, в том числе и японский. Японцы выводов из нее, однако, не сделали и полностью проиграли американцам сначала криптографическую, а потом и обычную войну на Тихом океане. Во время Второй мировой войны криптографией занимался выдающийся американский кибернетик Клод Шеннон. Именно в это время он заложил основы теории информации и теории связи в секретных системах.

В XX в. еще активнее теоретического развивался «прикладной криптоанализ», проще говоря, покупка или воровство шифров и шифромашин. Об успехах в этой области советских спецслужб много написано в книге Кана и недавно вышедшей у нас книге Б. Анина. Впрочем, и американцы не отставали. Об успехах советской теоретической криптографии Кан отзывается также высоко*, но по понятным причинам имен советских криптографов, за исключением некоторых, работавших в 20–30-е годы, он не называет. Вероятно, они останутся в области легенд**.

В 1970-е годы произошла криптографическая революция, выведшая криптографию из области секретности. Впервые был опубликован шифр в качестве стандарта (раньше это словосочетание было просто нелепостью!) — это американская криптосистема DES (первое название «Люцифер»). Она рекомендована для шифрования данных в компьютерах и другой электронной технике. В секрете надо хранить лишь

* В одной своей книге он дал такое определение великой державы: великая страна — это страна, имеющая ядерное оружие, межконтинентальные ракеты и криптографию.

** Впрочем, имена руководителей отделов, в подчинении которых находились криптографические службы, довольно широко известны, например, Глеб Бокий. Д. Кан написал о нем достаточно подробно, но далеко не все. Недавно Бокий стал, например, героем книги О. Шишкина «Битва за Гималаи» с подзаголовком «НКВД: магия и шпионаж», упоминается в книге А. Виноградова «Тайные битвы XX столетия» и др. Там рассказывается о тайных организациях мистико-масонского типа, в которые он был вхож, о странных экспедициях в Тибет (Тибетом почему-то интересовались и в гитлеровской Германии), о подчинявшихся ему лабораториях, занимавшихся телепатией, гипнозом и биоэнергетикой, и многим другим. Но, возможно, это все тоже легенды. Достоверно известно только, что он был расстрелян в 1937 г.

56-битный ключ *. Начали публиковаться в открытой печати и другие шифры, а также возможные атаки на них. Недавно прошел открытый (!) конкурс на замену этого стандарта, и уже утвержден новый стандарт **.

Тогда же, в 70-е годы, были придуманы первые шифровальные системы с открытым ключом, и начало развиваться немыслимое ранее научное направление. Начали издаваться специальные журналы и проводиться конференции.

Опишем одну из самых простых и самых популярных систем открытого шифрования — систему RSA (Ривеста—Шамира—Адлемана). Вся математика этой системы основана на теореме Эйлера, с помощью которой доказывается следующее утверждение.

Упражнение 55. Пусть $n = pq$, где p, q — различные простые, $\bar{s}, \bar{t} \in \mathbb{Z}_{\varphi(n)}^*$, $\bar{s}\bar{t} = \bar{1}$. Докажите, что отображения $x \rightarrow x^s$ и $x \rightarrow x^t$ являются изоморфизмами группы $\mathbb{Z}_n^*$, взаимно обратными друг другу.

Отображение $x \rightarrow x^s$ группы $\mathbb{Z}_n^*$ в себя можно использовать для так называемого открытого шифрования. Шифровка производится очень быстро с помощью компьютера, числа s и n можно сообщить всем желающим. Дешифровка также проводится быстро, если известен ключ t . Проводящему атаку на эту систему для нахождения t из сравнения $st \equiv 1 \pmod{\varphi(n)}$ надо знать $\varphi(n) = (p-1)(q-1) = n+1-p-q$, т.е. p и q . Вы выбираете p и q очень большими, сообщаете всем $n = pq$ и произвольное s , $(s, \varphi(n)) = 1$, и можете быть уверенными, что пока не будет изобретен алгоритм быстрого разложения на простые, ваша секретная система будет надежной.

Некоторые замечания об использовании этой системы и примеры других подобных систем приведены в следующих далее упражнениях.

Задачи и упражнения к § 2.9

1*. (Криптографическая лемма.) В условиях предыдущего упражнения докажите, что отображения $x \rightarrow x^s$ и $x \rightarrow x^t$ являются взаимно однозначными и взаимно обратными не только на подгруппе $\mathbb{Z}_n^*$, но и на всем кольце вычетов $\mathbb{Z}_n$.

У к а з а н и е. Примените китайскую теорему об остатках.

* Разработчики этого алгоритма из ИВМ предлагали вначале 128-битный ключ, но под давлением АНБ — Агентства национальной безопасности — длина ключа была уменьшена. Интересно, почему?

** Возможно, в АНБ уже смирились с тем, что криптография выходит из-под контроля спецслужб, но экспорт качественных криптографических алгоритмов из США в другие страны запрещен.

2*. Докажите, что отображение $x \rightarrow f(x) = x^s \bmod n$ всегда имеет 4 неподвижных точки в множестве $\mathbb{Z}_n^*$ и девять неподвижных точек в множестве $\mathbb{Z}_n$ (неподвижная точка отображения — это такое число a , которое переходит в себя при этом отображении).

У к а з а н и е. Примените китайскую теорему об остатках.

3*. Докажите, что если $s - 1$ будет общим кратным чисел $p - 1$ и $q - 1$, то отображение $x \rightarrow f(x) = x^s \bmod n$ будет тождественным.

Заметим, что для предотвращения очевидных атак на эту систему рекомендуется:

а) не выбирать числа p и q слишком близкими друг к другу (рекомендуется, чтобы их двоичные записи отличались по длине на несколько разрядов), иначе облегчается возможность факторизации числа n ;

б) следить за тем, чтобы число $p - 1$ не было делителем числа $q - 1$ и наоборот, и вообще чтобы эти числа не имели бы большого общего делителя, так как тогда возникает возможность найти ключ t перебором;

в) не допускать того, чтобы в разложении $\varphi(n)$ на множители встречались только малые простые числа (по той же причине).

Для надежности можно было бы использовать только так называемые *безопасные* простые числа, т. е. такие числа p , для которых и число $(p - 1)/2$ тоже простое. К сожалению, проблема генерации таких чисел трудна, и до сих пор неизвестно, конечно или бесконечно их количество.

Заметим еще, что не рекомендуется использовать слишком малые числа s и t (так как тогда опять появляется возможность нахождения ключа перебором, но в случае малого s для этого, правда, нужно суметь перехватить одинаковое сообщение, посланное многим разным получателям), а также такие числа s , что $s - 1$ будет общим кратным чисел $p - 1$ и $q - 1$, например, $s = \varphi(n)/2 + 1$, так как тогда зашифрованный текст всегда просто совпадает с незашифрованным. Кроме того, во всех случаях надо следить, чтобы случайно не попасть в «неподвижную точку».

4*. (Общий секретный ключ.) Нахождение индекса произвольного элемента из $\mathbb{Z}_p$ относительно заданного первообразного корня a (называемое коротко *дискретным логарифмированием*) требует весьма громоздких вычислений, и при p , состоящем из нескольких сотен цифр, не под силу и суперЭВМ. Лишь в случае, когда $p - 1$ имеет только малые простые множители, известен сравнительно быстро работающий алгоритм дискретного логарифмирования.

На предположении о труднорешаемости задачи дискретного логарифмирования основана следующая система Диффи—Хеллмана* *открытого распределения ключей*. Допустим, что A и B хотят, пользуясь

* У. Диффи и М. Хеллман — современные американские математики.

публичными каналами связи (например, электронной почтой), выработать общую секретную информацию (*общий ключ*). Противник знает о затеях A и B и может перехватывать весь их обмен информацией.

Предложите протокол выработки общего ключа, роль которого играет некоторый элемент из $\mathbb{Z}_p^*$, причем для его выработки требуется обмениваться двумя элементами из $\mathbb{Z}_p^*$. Каждый из партнеров вычисляет свой элемент, пользуясь своим ключом (секретным элементом), а потом, получив вычисленный партнером элемент, с помощью того же ключа вычисляет общий ключ (он, разумеется, должен получиться одинаковым у обоих). Алгоритм вычисления общего ключа должен быть простым, а алгоритм взлома этой системы (конечно, при отсутствии информации о ключах партнеров) — очень трудоемким.

У к а з а н и е. Возьмите в поле $\mathbb{Z}_p$ какой-нибудь первообразный корень g и воспользуйтесь тождеством $(g^n)^m = (g^m)^n$.

5*. (Алгоритм Гельфонда дискретного логарифмирования.) Дискретный логарифм в конечном поле порядка q можно вычислить, сделав не более $C\sqrt{q} \log_2 q$ операций деления и не более $C\sqrt{q} \log_2 q$ операций сравнения элементов поля.

6*. (Разделение секретного ключа на части.) Допустим, что вам поручили организовать доступ к секретной информации на компьютере для трех сотрудников банка так, чтобы они, только собравшись втроем, смогли получить ее. Каждому вы сообщаете ключ — некоторое большое (например, стозначное) число, которое он хранит в секрете от остальных. Паролем, который открывает секретную информацию, является неизвестное никому из них число, которое, однако, можно быстро определить (разумеется, с помощью компьютера) по трем упомянутым ключам. В случае же отсутствия одного из них для определения пароля придется (даже зная алгоритм определения пароля по ключам) перебрать $9 \cdot 10^{99}$ вариантов возможного значения неизвестного ключа (а это пока не доступно даже суперЭВМ). Кроме того, для надежности вы можете периодически менять ключи. Это смогут сделать даже сами работники банка (договорившись только о размерах ключей, чтобы гарантировать их отличие друг от друга, и выбирая в качестве ключей, например, числа вида $2^{2^n} + 1$), и сохранить пароль в тайне даже от вас.

Предложите алгоритм определения пароля по ключам, основанный на применении китайской теоремы об остатках.

У к а з а н и е. Следующий алгоритм принадлежит Шамиру*. Выберем 3 больших попарно взаимно простых числа, например, числа Ферма $a_1 = 2^{2^n} + 1$, $a_2 = 2^{2^{n+1}} + 1$, $a_3 = 2^{2^{n+2}} + 1$. Пусть i -й «компаньон»

* А. Шамир — современный израильский математик.

в качестве ключа выбирает произвольное число k_i в пределах от 1 до $a_i - 1$. Тогда, собравшись вместе, они могут выработать пароль k , взяв в качестве него такое число в пределах от 1 до $a - 1$, $a = a_1 a_2 a_3$, которое при делении на a_i дает в остатке k_i . Как было показано в этом параграфе, число k можно вычислить по формуле $k = k' - [k'/a]a$, где

$$k' = k_1 n_1 + k_2 n_2 + k n_3, \quad n_i m_i - a_i q_i = 1, \quad m_i = a_j a_k, \quad j \neq k \neq i \neq j.$$

Для вычисления n_i можно применить алгоритм Евклида. Нетрудно написать программу для компьютера, которая будет вычислять пароль k после того, как «компаньоны», таясь друг от друга, введут в него свои ключи. Положим $N = 2^n$. Если двое, в тайне от третьего, захотят найти ключ k , то им придется перебрать все возможные варианты выбора третьего ключа (потому что разным способам выбора ключей соответствуют разные значения k), т. е. перебрать не менее 2^N вариантов.

7*. Предложите алгоритм разделения секрета со свойствами, аналогичными предыдущему, но основанный на лагранжевой интерполяции.

Глава III. Многочлены

§ 3.1. Кольцо многочленов

Возьмем произвольное кольцо K и назовем *многочленом* над этим кольцом формальную сумму

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0,$$

где элементы $a_0, a_1, \dots, a_{n-1}, a_n$, $n \geq 0$, принадлежат кольцу K , а x — не входящий в кольцо символ *переменной*.

Определение 65. Элементы кольца $a_0, \dots, a_n$ называются *коэффициентами* многочлена. Будем рассматривать только многочлены, у которых старший коэффициент a_n *отличен от нуля*.

Степенью многочлена называется в этом случае число n , обозначаемое далее как $\deg f(x)$.

Элементы кольца K , не равные 0, будем рассматривать как *многочлены нулевой степени*. Нуль также считаем многочленом. Степень у нулевого многочлена *не определена*.

Определение 66. Многочлены

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0,$$

$$g(x) = b_m x^m + a_{m-1} x^{m-1} + \dots + b_1 x + b_0$$

называются *равными*, если $m = n$ и равны все коэффициенты при соответствующих степенях переменной, т. е. $a_i = b_i$, $i = 0, 1, \dots, n$.

Определим арифметические операции на множестве многочленов $K[x]$ с коэффициентами из кольца K .

Определение 67. Назовем *суммой* многочленов

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0,$$

$$g(x) = b_m x^m + a_{m-1} x^{m-1} + \dots + b_1 x + b_0$$

многочлен $h(x)$, коэффициент которого при x^i равен $c_i = a_i + b_i$ для любого $i = 0, 1, \dots, \max\{n, m\}$.

Если один или несколько старших коэффициентов у рассматриваемой суммы равны нулю (а это возможно лишь при $n = m$), то они просто

удаляются из нее, так, чтобы старший из оставшихся коэффициентов был отличен от нуля. Многочлен, имеющий только один ненулевой коэффициент, называется *одночленом*. Аналогично определяются двучлены и трехчлены.

Определение 68. *Произведением* многочленов

$$\begin{aligned} f(x) &= a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0, \\ g(x) &= b_m x^m + a_{m-1} x^{m-1} + \dots + b_1 x + b_0 \end{aligned}$$

называется многочлен $h(x)$, коэффициент которого при x^i равен

$$d_i = \sum_{j+k=i} a_j b_k.$$

З а м е ч а н и е. Указанную сумму можно понимать и как сумму

$$d_i = \sum_{j=0}^n a_j b_{i-j},$$

если условиться, что все входящие в нее коэффициенты с индексами, не лежащими в пределах от 0 до n , равны нулю.

Теорема 57. *Множество всех многочленов над кольцом K — кольцо.*

Д о к а з а т е л ь с т в о. Нулевым элементом кольца многочленов является нулевой многочлен, отождествляемый с нулем кольца K , а единичным — единица кольца K .

Обратным элементом для произвольного многочлена

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

относительно операции сложения является многочлен

$$-f(x) = (-a_n) x^n + (-a_{n-1}) x^{n-1} + \dots + (-a_1) x + (-a_0),$$

получающийся из исходного «сменой знака» у всех коэффициентов. Поэтому *вычитание* многочленов осуществляется так же, как и сложение, но с заменой операции сложения коэффициентов на операцию вычитания.

Выполнение аксиом коммутативной группы относительно операции сложения непосредственно вытекает из справедливости этих аксиом для кольца коэффициентов, которое, кстати, можно считать содержащимся в соответствующем кольце многочленов.

Легко видеть, что каждый многочлен равен сумме всех своих одночленов.

Аксиома дистрибутивности (другими словами, распределительный закон умножения относительно сложения) для кольца многочленов легко следует из тождеств

$$\sum_{j+k=i} a_j(b_k + c_k) = \sum_{j+k=i} a_j b_k + \sum_{j+k=i} a_j c_k,$$

а аксиома ассоциативности умножения для кольца многочленов легко следует из аксиомы дистрибутивности, если с ее помощью выполнять умножение многочленов, разбивая их на суммы одночленов и складывая потом получившиеся произведения одночленов, для которых выполнение ассоциативного закона относительно умножения очевидно. $\square$

Теорема 58. *Степень суммы многочленов над кольцом не превосходит наибольшей из степеней слагаемых.*

Доказательство. Для двух слагаемых это очевидно из определения операции сложения. Для случая многих слагаемых это легко доказывается по индукции. $\square$

Напомним, что *областью целостности* называется кольцо без делителей нуля.

Упражнение 56. Докажите, что

- а) кольцо целых чисел является областью целостности;
- б) любое поле также является областью целостности.

Теорема 59. *В кольце многочленов над областью целостности степень произведения ненулевых многочленов равна сумме степеней сомножителей.*

Доказательство. Доказательство для случая двух сомножителей следует из определения умножения многочленов: наибольшая возможная степень x в произведении многочленов $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$, $a_n \neq 0$, и $g(x) = b_m x^m + a_{m-1} x^{m-1} + \dots + b_1 x + b_m$, $b_m \neq 0$, равна $n + m$, т.к. $a_0 b_0 \neq 0$ согласно свойству области целостности. Для случая нескольких сомножителей это легко доказывается по индукции. $\square$



Если в кольце K есть делители нуля, то теорема 59 неверна.

Упражнение 57. Например, если $K = \mathbb{Z}_6$, то $\bar{3}x \cdot \bar{2}x = \bar{0}$, и в этом случае степень произведения меньше суммы степеней сомножителей. Для произвольного кольца коэффициентов степень произведения не больше суммы степеней сомножителей.

Определение 69. Если для многочленов $f(x)$ и $g(x) \neq 0$ справедливо разложение $f(x) = g(x) \cdot h(x) + r(x)$, где $h(x)$ и $r(x)$ — некоторые другие многочлены, причем $\deg r(x) < \deg g(x)$, то $h(x)$ называется *частным*, а $r(x)$ — *остатком*.

Теорема 60 (о делении с остатком). Для любых многочленов $f(x)$ и $g(x) \neq 0$ над произвольным полем F частное и остаток существуют и определены однозначно как многочлены над тем же полем F .

Доказательство. Существование частного и остатка очевидно в случае $\deg f(x) < \deg g(x)$.

В случае $\deg f(x) \geq \deg g(x)$ применим для их нахождения следующий алгоритм деления с остатком.

Предположим, что $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ и $g(x) = b_m x^m + a_{m-1} x^{m-1} + \dots + b_1 x + b_0$, тогда $f(x) - \frac{a_n}{b_m} x^{n-m} g(x) = h(x)$, причем $\deg h(x) < n$. Затем поделим $h(x)$ на $g(x)$ и т.д. Процедура закончится, так как на каждом шаге будет понижаться степень разности до тех пор, пока она не станет меньше $m = \deg g(x)$. Тогда получим, что $f(x) = g(x) \cdot \varphi(x) + r(x)$, причем $\deg r(x) < \deg g(x)$.

Доказательство единственности проведем от противного. Пусть

$$f(x) = g(x) \cdot h_1(x) + r_1(x) = g(x) \cdot h_2(x) + r_2(x),$$

тогда $g(x) \cdot (h_1(x) - h_2(x)) = r_2(x) - r_1(x)$. Если бы $h_1(x) - h_2(x) \neq 0$, то степень левой части была бы больше степени правой. То есть $h_1(x) = h_2(x)$, а значит, и $r_1(x) = r_2(x)$. Противоречие. $\square$

З а м е ч а н и е. Для доказательства единственности требуется, по крайней мере, чтобы кольцо коэффициентов было областью целостности. Для доказательства существования в случае, если K не поле, достаточно считать, что старший коэффициент $g(x)$ равен 1.

Далее у нас изредка будут встречаться *многочлены от нескольких переменных*. Определения основных понятий в этом случае, как правило, являются естественными обобщениями соответствующих определений для одной переменной.

Назовем *многочленом над кольцом K от переменных $x_1, \dots, x_n$* конечную формальную сумму

$$f(x) = \sum_{i_1, \dots, i_n \geq 0} a_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n},$$

где коэффициенты $a_{i_1 \dots i_n}$ принадлежат кольцу K , а $x_1, \dots, x_n$ — не входящие в кольцо символы переменных.

Определение 70. Многочлены

$$f(x) = \sum_{i_1, \dots, i_n \geq 0} a_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n}, \quad g(x) = \sum_{i_1, \dots, i_n \geq 0} b_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n}$$

называются *равными*, если попарно равны все их коэффициенты

$$a_{i_1 \dots i_n} = b_{i_1 \dots i_n}.$$

Определение 71. Многочлен, имеющий только один ненулевой коэффициент, называется *одночленом*. *Степенью одночлена* называется сумма степеней всех его переменных. *Степенью многочлена* называется *максимальная* из степеней всех его одночленов. Одночлены с максимальной степенью называются *старшими одночленами*. Так же называются их коэффициенты.



Старших одночленов может быть несколько.

Примеры. 1. Многочлен $x_1^2 + x_1x_2 + x_2^2$ — неполный квадрат суммы.
2. Если переменных немного, то стараются обходиться без индексов: $x^2 + xy + y^2$.

Будем рассматривать только многочлены, у которых старшие коэффициенты *отличны от нуля*.

Элементы кольца K , не равные 0, будем рассматривать как *многочлены нулевой степени*. Степень у нулевого многочлена не определена.

Множество всех определенных выше многочленов от переменных $x_1, \dots, x_n$ обозначают $K[x_1, \dots, x_n]$. Определим арифметические операции на этом кольце.

Определение 72. Назовем *суммой* многочленов

$$f(x) = \sum_{i_1, \dots, i_n \geq 0} a_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n}, \quad g(x) = \sum_{i_1, \dots, i_n \geq 0} b_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n}$$

многочлен

$$f(x) + g(x) = \sum_{i_1, \dots, i_n \geq 0} (a_{i_1 \dots i_n} + b_{i_1 \dots i_n}) x_1^{i_1} \dots x_n^{i_n},$$

а *произведением* — многочлен, получающийся из суммы

$$f(x)g(x) = \sum_{i_1, j_1, \dots, i_n, j_n \geq 0} a_{i_1 \dots i_n} b_{j_1 \dots j_n} x_1^{i_1+j_1} \dots x_n^{i_n+j_n}$$

приведением подобных членов.

Примеры. 1. $x^2 - y^2 = (x - y)(x + y)$.

2. $x^3 - y^3 = (x - y)(x^2 + xy + y^2)$.

3. $x^3 + y^3 = (x + y)(x^2 - xy + y^2)$.

4. $x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + \dots + xy^{n-2} + y^{n-1})$.

5. $x^{2n+1} + y^{2n+1} = (x + y)(x^{2n} - x^{2n-1}y + \dots - xy^{2n-1} + y^{2n})$.

6. Еще примерами могут служить биномиальная и полиномиальная теоремы.

Аналогично случаю одной переменной доказывается следующая теорема.

Теорема 61. Множество многочленов $K[x_1, \dots, x_n]$ образует целое кольцо относительно операций сложения и умножения.

Нулевым элементом кольца многочленов является нулевой многочлен, отождествляемый с нулем кольца K , а единичным — единица кольца K .

Обратным элементом для произвольного многочлена $f(x)$ относительно операции сложения является многочлен, получающийся из исходного сменой знака у всех коэффициентов. Каждый многочлен равен сумме всех своих одночленов.

Степень суммы многочленов над кольцом не превосходит наибольшей из степеней слагаемых.

Теорема 62. В кольце многочленов над областью целостности степень произведения ненулевых многочленов равна сумме степеней сомножителей.

Верна также

Теорема 63. Кольца $K[x_1, \dots, x_n]$ и $(K[x_1, \dots, x_{n-1}])[x_n]$ изоморфны.

Доказательство. Для установления изоморфизма достаточно представить любой многочлен

$$f(x) = \sum_{i_1, \dots, i_n \geq 0} a_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n}$$

как многочлен от одной переменной x_n

$$f(x) = \sum_{i_n \geq 0} \left(\sum a_{i_1 \dots i_n} x_1^{i_1} \dots x_{n-1}^{i_{n-1}} \right) x_n^{i_n},$$

но с коэффициентами из кольца $K[x_1, \dots, x_{n-1}]$. Например,

$$x_1^2 x_2 + x_1 x_2 + x_1 x_2^2 = x_1(x_2 + x_2^2) + x_1^2(x_2),$$

при этом степень полученного многочлена от x_n называется степенью по x_n исходного многочлена от переменных $x_1, \dots, x_n$. $\square$

Упражнение 58. Докажите аккуратно последние три теоремы.



Деление с остатком на многочлены нескольких переменных так просто не переносится.

Задачи и упражнения к § 3.1

В этом цикле задач рассматриваем только многочлены над полем рациональных чисел.

1. Найдите сумму коэффициентов многочлена $(1 - 1998x + 1999x^2)^{2001}$.
2. Сравнить коэффициенты при x^{1994} в многочленах
 - а) $(1 - 1994x + 1993x^2)^{2000}$ и $(1 + 1994x + 1993x^2)^{2000}$;
 - б) $(1 - 1994x^2 + 1993x^3)^{2000}$ и $(1 + 1994x^2 + 1993x^3)^{2000}$.
3. Найдите коэффициент при x^{50} в многочлене

$$(1+x)^{1000} + x(1+x)^{999} + \dots + x^{999}(1+x) + x^{1000}.$$
4. Найдите остаток от деления $x + x^3 + x^9 + \dots + x^{3^n}$ на: а) $x - 1$;
б) $x^2 - 1$.
5. Многочлен при делении на $x - a$ дает остаток b , а при делении на $x - c$ — остаток d . Какой остаток будет при делении на $(x - a)(x - c)$?
- 6*. Найдите коэффициент при x^{14} в частном от деления $x^{1994} - 1$ на

$$x^4 + x^3 + 2x^2 + x + 1.$$

У к а з а н и е. Сначала поделить с остатком на $x^{12} - 1$, а потом умножить на многочлен

$$\frac{x^{12} - 1}{x^4 + x^3 + 2x^2 + x + 1}.$$

7*. Найдите все многочлены $P(x)$, для которых справедливо тождество

$$xP(x - 1) = (x - 26)P(x).$$

8*. Пусть $f(x) = 1 + x + x^2 + x^3 + x^4$. Найдите остаток от деления $f(x^5)$ на $f(x)$.

9*. Многочлен $P(x)$ с а) натуральными; б) целыми коэффициентами при любом n принимает натуральное значение с суммой десятичных цифр $s(n)$. Докажите, что последовательность $s(n)$ содержит бесконечно много одинаковых чисел.

10. Многочлен от двух переменных $x^{1994}y^{1994} + 1$ нельзя представить в виде произведения двух многочленов от переменных x и y соответственно.

11. Разделить многочлен

а) $(x + 1)^{2n} - x^{2n} - 2x - 1$ на $x(x + 1)(2x + 1)$;

б) $nx^{n+1} - (n + 1)x^n + 1$ на $(x - 1)^2$.

12. Если $x - 1$ делит $P(x^n)$, то $x^n - 1$ делит $P(x^n)$.

13*. При каком целом a многочлен $x^{13} + x + 90$ делится на $x^2 - x + a$?

§ 3.2. Алгоритм Евклида и теорема Безу

Для простоты далее будем считать, что кольцо коэффициентов K есть либо $\mathbb{Z}$ — кольцо целых чисел, либо F — поле.

Пусть многочлены $f(x)$ и $g(x)$ принадлежат кольцу $K[x]$.

Определение 73. Многочлен $f(x)$ *делится* на $g(x)$, если существует такой многочлен $a(x) \in K[x]$, что $f(x) = g(x) \cdot a(x)$ (обозначение $g(x) \mid f(x)$).

Другими словами, многочлен $f(x)$ *делится* на $g(x)$, если остаток от деления равен нулю.

Справедливы следующие очевидные свойства отношения делимости:

- 1) если $f(x)$ делится на $g(x)$, а $g(x)$ делится на $h(x)$, то $f(x)$ делится на $h(x)$;
- 2) если $f(x)$ и $g(x)$ делятся на $h(x)$, то $u(x)f(x) + v(x)g(x)$ делится на $h(x)$.

Определение 74. Многочлен $d(x)$ называется *наибольшим общим делителем* (НОД) многочленов $f(x)$ и $g(x)$, если каждый из них делится на $d(x)$ и любой их общий делитель делит $d(x)$, причем будем считать для определенности старший коэффициент $d(x)$ равным 1.

Для НОД будем использовать обозначение $d(x) = (f(x), g(x))$.

Используя теорему о делении с остатком, можно для нахождения НОД двух многочленов над заданным полем коэффициентов применить алгоритм Евклида аналогично тому, как это делалось для целых чисел:

$$f(x) = g(x) \cdot q_0(x) + r_1(x), \text{ где } 0 \leq \deg r_1(x) < \deg g(x),$$

$$(f(x), g(x)) = (g(x), r_1(x))$$

$$g(x) = r_1(x) \cdot q_1(x) + r_2(x), \text{ где } 0 \leq \deg r_2(x) < \deg r_1(x),$$

$$(f(x), g(x)) = (g(x), r_1(x)) = (r_1(x), r_2(x)),$$

$$r_1(x) = r_2(x) \cdot q_2(x) + r_3(x), \text{ где } 0 \leq \deg r_3(x) < \deg r_2(x),$$

$$(f(x), g(x)) = (r_1(x), r_2(x)) = (r_2(x), r_3(x)),$$

.....

$$r_{n-2}(x) = r_{n-1}(x) \cdot q_{n-1}(x) + r_n(x), \text{ где } 0 \leq \deg r_n(x) < \deg r_{n-1}(x),$$

$$(f(x), g(x)) = (r_{n-2}(x), r_{n-1}(x)) = (r_{n-1}(x), r_n(x)),$$

$$r_{n-1}(x) = r_n(x) \cdot q_n(x),$$

$$(f(x), g(x)) = (r_{n-1}(x), r_n(x)) = r_n(x).$$

Осуществимость и однозначность этого процесса последовательного деления обосновывается теоремой о делении с остатком.

Аналогично соответствующей теореме о НОД чисел доказывается следующая теорема о линейном представлении НОД многочленов.

Теорема 64. Для любых многочленов $f(x)$, $g(x)$ над произвольным полем F существуют такие многочлены $a(x)$, $b(x) \in F[x]$, что

$$d(x) = a(x)f(x) + b(x)g(x).$$

Доказательство. Индукцией по i проверяем, что

$$r_i(x) = u_i(x)f(x) + v_i(x)g(x).$$

Подобно числовому случаю, алгоритм Евклида для многочленов можно расширить так, чтобы он вычислял не только последовательность $r_i(x)$, но и последовательности $u_i(x)$, $v_i(x)$, а значит, и линейное представление НОД. $\square$

Определение 75. Каждому многочлену $f(x) \in K[x]$ можно сопоставить реализуемую им *полиномиальную функцию* $\tilde{f}: K \rightarrow K$, определяемую равенством

$$\tilde{f}(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0,$$

где $a_n, a_{n-1}, \dots, a_1, a_0$ — его коэффициенты.

Легко проверить, что сумме многочленов соответствует сумма реализуемых ими полиномиальных функций, а произведению — произведение этих же функций.

Определение 76. Корнем многочлена $f(x) \in K[x]$ называется любой такой элемент $\alpha \in K$, что $f(\alpha) = 0$.

Теорема 65 (Безу). Для любого $f(x) \in K[x]$, $\deg f(x) \geq 1$, и для любого корня $\alpha \in K$ данного многочлена $f(x)$ справедливо равенство $f(x) = (x - \alpha)g(x)$.

Доказательство. Выполняя деление с остатком, получаем, что для любого $f(x) \in K[x]$, $\deg f(x) \geq 1$, и для любого $\alpha \in K$ справедливо равенство $f(x) = (x - \alpha)g(x) + r$, где $r \in K$. Подставляя в него $x = \alpha$, имеем $r = 0$. $\square$

Теорема 66 (о числе корней). Любой многочлен $f(x)$ степени n над областью целостности K имеет не более n корней.

Доказательство. База индукции ($n = 1$) очевидна. Выполним шаг индукции.

Пусть теорема верна для многочленов степени $n - 1$. Если многочлен $f(x)$ степени n не имеет корней в K , то утверждение очевидно верно.

Если α_1 — корень $f(x)$, то $f(x) = (x - \alpha_1)h(x)$ согласно теореме Безу. Пусть α_2 — корень многочлена $f(x)$ и $\alpha_1 \neq \alpha_2$, тогда $f(\alpha_2) = (\alpha_2 - \alpha_1)h(\alpha_2) = 0$ и $\alpha_2 - \alpha_1 \neq 0$, но в области целостности нет делителей нуля, следовательно, $h(\alpha_2) = 0$, а $h(x)$ имеет не более $n - 1$ корней по предположению индукции, значит, многочлен $f(x)$ имеет не более n корней. $\square$

Следствие из теоремы 66. Если многочлен $f(x)$ степени n с коэффициентами из области целостности K имеет в ней n корней, то его можно представить в виде произведения элемента из K на n линейных множителей с коэффициентами из K .

З а м е ч а н и е.



Утверждение теоремы неверно в том случае, если кольцо K не является областью целостности.

Упражнение 59. Квадратный двучлен $x^2 - 1$ имеет в кольце $\mathbb{Z}_8$ четыре корня ($\bar{1}$, $\bar{3}$, $\bar{5}$, $\bar{7}$).

Теорема 67 (о полиномиальных функциях). Пусть область целостности K бесконечна и два многочлена $f_1(x)$ и $f_2(x)$ над K принимают одинаковые значения при всех $s \in K$, т. е. равны как функции. Тогда эти многочлены совпадают друг с другом.

Доказательство. Рассуждаем от противного. Пусть степень многочлена $F(x) = f_1(x) - f_2(x)$ равна n . Из условия теоремы следует, что можно выбрать $n + 1$ элементов из K , которые являются корнями этого многочлена. Тем самым получено противоречие с теоремой 66. $\square$

Из доказанной теоремы вытекает, что по известным значениям многочлена степени n в $n + 1$ различных точках многочлен определяется однозначно.

Однако не сразу ясно, как его выразить в явном виде. Если область целостности является полем, то для этого можно использовать интерполяционный многочлен Лагранжа, о котором пойдет речь в следующем параграфе.

Задачи и упражнения к § 3.2

1. Многочлен $x^3 \in \mathbb{Z}_8[x]$ имеет в $\mathbb{Z}_8$ четыре корня и четыре разных разложения на неприводимые (т. е. неразложимые далее) множители в $\mathbb{Z}_8[x]$.

2. Если $f(x)$ и $g(x) \in F[x]$, где F — поле, и степень $f(x)$ не меньше степени $g(x)$, то $f(x)$ однозначно представим в виде $f = f_0 + f_1 g + \dots + f_d g^d$, где степени f_i меньше степени g .

3. Число корней многочлена $f(x) \in F[x]$ в поле F не превосходит его степени, даже если каждый корень считать столько раз, какова его кратность.

4. Разложите на множители $x^5 + x^3 + x + 1$ над полем $\mathbb{Z}_2$.

5. Найдите $(x^5 + x^4 + 1, x^4 + x^2 + 1)$ над полем $\mathbb{Z}_2$.

6. Найдите $(x^5 + x^4 + 1, x^4 + x^2 + 1)$ над полем $\mathbb{Q}$.

Далее все многочлены рассматриваются над полем $\mathbb{Q}$.

7. Применяя алгоритм Евклида, найдите такие многочлены M_1 и M_2 , что $(x^4 - 4x^3 + 1)M_1(x) + (x^3 - 3x^2 + 1)M_2(x) = 1$.

8*. Применяя алгоритм Евклида, найдите $(x^n + a^n, x^m + a^m)$.

9. Применяя алгоритм Евклида, докажите, что

$$(x^n - 1, x^m - 1) = x^{(n,m)} - 1.$$

10. Применяя алгоритм Евклида, докажите, что при $k \mid (n, m)$

$$\left(\frac{x^n - 1}{x^k - 1}, \frac{x^m - 1}{x^k - 1} \right) = \frac{x^{(n,m)} - 1}{x^k - 1}.$$

11. (Гаусс.) Докажите, что все рациональные корни многочлена

$$f(x) = a_n x^n + \dots + a_0$$

с целыми коэффициентами имеют вид $\pm p/q$, где

$$p \mid a_0, \quad q \mid a_n, \quad (p - mq) \mid f(m).$$

§ 3.3. Интерполяция

Пусть дана таблица значений многочлена степени n над полем F

x	x_0	x_1	$\dots$	x_k	$\dots$	x_{n-1}	x_n
$f(x)$	y_0	y_1	$\dots$	y_k	$\dots$	y_{n-1}	y_n

где $x_1, \dots, x_k$ — различные, а $y_1, \dots, y_k$ — необязательно различные элементы поля F .

Определение 77. Многочлены

$$l_n^k(x) = \frac{(x - x_0)(x - x_1) \dots (x - x_{k-1})(x - x_{k+1}) \dots (x - x_{n-1})(x - x_n)}{(x_k - x_0)(x_k - x_1) \dots (x_k - x_{k-1})(x_k - x_{k+1}) \dots (x_k - x_{n-1})(x_k - x_n)},$$

где $k = 0, \dots, n$, называются *фундаментальными многочленами Лагранжа*.

Справедлива следующая лемма.

Лемма 19. Для $x = x_0, \dots, x_n$

$$l_n^k(x) = \begin{cases} 1, & \text{если } x = x_k, \\ 0, & \text{если } x \neq x_k. \end{cases}$$

Доказательство. Непосредственно проверяется, что при $x \neq x_k$ числитель дроби, определяющей многочлен, обращается в нуль, а при $x = x_k$ этот числитель не равен нулю и совпадает со знаменателем. $\square$

Определение 78. Многочлен степени n

$$f(x) = y_0 l_n^0(x) + y_1 l_n^1(x) + \dots + y_n l_n^n(x)$$

называется *интерполяционным многочленом Лагранжа**, соответствующим данной таблице значений.

Теорема 68 (интерполяционная формула). Интерполяционный многочлен Лагранжа $f(x)$ принимает значения, указанные в данной таблице, т. е. решает задачу интерполяции.

Доказательство. Из леммы следует, что при $x = x_k$

$$y_k l_n^k(x) = y_k,$$

а все остальные слагаемые определяющей многочлен суммы обращаются в нуль. Поэтому вся сумма тогда равна y_k , т. е. $f(x_k) = y_k$. $\square$

Упражнение 60. Проверьте, что вычисление коэффициентов интерполяционного многочлена по формуле Лагранжа—Варинга требует n сложений, $2n^2 + 2n$ вычитаний, $2n^2 + n - 1$ умножений и $n + 1$ делений.



Для многочленов над конечными полями последняя теорема предыдущего параграфа неверна.

Пусть $\mathbb{Z}_p$ — поле вычетов по модулю p , где p — простое число, а многочлен $f(x) \in \mathbb{Z}_p[x]$.

Тогда справедлива (предлагавшаяся в § 2.8 в виде задачи)

Теорема 69. Уравнение $f(x) = 0$, $f(x) \in \mathbb{Z}_p[x]$, равносильно уравнению степени не выше $p - 1$, другими словами, для любого многочлена $f(x) \in \mathbb{Z}_p[x]$ найдется многочлен степени не выше $p - 1$, значения которого для любого $x \in \mathbb{Z}_p$ совпадают со значениями многочлена $f(x)$.

Доказательство. Согласно теореме о делении с остатком можно записать, что

$$f(x) = (x^p - x)g(x) + r(x), \quad \text{где} \quad \deg r(x) \leq p - 1.$$

* Этот многочлен был открыт также английским математиком XVIII в. Э. Варингом (Eduard Waring, 1734–1798).

Но $x^p - x = 0$ для любого $x \in \mathbb{Z}_p$ согласно малой теореме Ферма. Значит, уравнение $f(x) = 0$ равносильно уравнению $r(x) = 0$, и справедливо тождество $f(x) = r(x)$. $\square$

Поэтому над полем $\mathbb{Z}_p$ задача интерполяции осмыслена только для многочленов степени, меньшей p . Но для таких многочленов она решается точно так же, как и для бесконечных полей. В частности, из теоремы Лагранжа вытекает следующая теорема.

Теорема 70. *Для любого отображения $g: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ найдется многочлен $f(x)$ степени не выше $p - 1$, реализующий эту функцию, т. е. такой, что для любого $x \in \mathbb{Z}_p$ справедливо равенство $f(x) = g(x)$, причем этот многочлен определен однозначно среди многочленов степени не выше $p - 1$.*

Доказательство. Существование этого многочлена вытекает из теоремы Лагранжа, а единственность фактически была доказана в последней теореме предыдущего параграфа. $\square$

Предыдущую теорему можно обобщить и на функции нескольких переменных.

В частности, справедлива следующая теорема.

Теорема 71. *Для любой функции $g(x_1, \dots, x_n)$, переменные и значения которой принадлежат полю $\mathbb{Z}_p$, найдется многочлен $f(x_1, \dots, x_n)$ от n переменных степени не выше $p - 1$, по каждой переменной реализующий эту функцию, т. е. такой, что для любого набора $(x_1, \dots, x_n) \in \mathbb{Z}_p^n$ справедливо равенство $f(x_1, \dots, x_n) = g(x_1, \dots, x_n)$, причем этот многочлен определен однозначно среди многочленов указанного вида.*

Доказательство. Сначала реализуем указанными многочленами функции, которые всюду равны нулю, кроме одной точки. Пусть, например, функция $\delta_{k_1, \dots, k_n}(x_1, \dots, x_n)$ равна единице при $(x_1, \dots, x_n) = (k_1, \dots, k_n)$, а в остальных случаях равна нулю. Для каждого $i = 1, \dots, n$ возьмем многочлен $f_i^{k_i}(x_i)$ степени $p - 1$ от переменной x_i , который равен единице при $x_i = k_i$ и нулю в остальных случаях, существование которого доказано в предыдущей теореме. Тогда многочлен, равный их произведению

$$f_{k_1, \dots, k_n}(x_1, \dots, x_n) = f_1^{k_1}(x_1) \dots f_n^{k_n}(x_n),$$

будет равен единице при $(x_1, \dots, x_n) = (k_1, \dots, k_n)$ и нулю в остальных случаях, т. е.

$$f_{k_1, \dots, k_n}(x_1, \dots, x_n) = \delta_{k_1, \dots, k_n}(x_1, \dots, x_n).$$

Если же функция $\delta_{k_1, \dots, k_n}(x_1, \dots, x_n)$ в точке $(k_1, \dots, k_n)$ равна не единице, а некоторому значению $a \in \mathbb{Z}_p$, а в остальных точках равна нулю, то многочлен $f_{k_1, \dots, k_n}(x_1, \dots, x_n)$ после умножения на a опять будет реализовывать эту функцию.

Произвольная функция $g(x_1, \dots, x_n)$ реализуется многочленом, равным сумме всех многочленов $g(k_1, \dots, k_n)f_{k_1, \dots, k_n}(x_1, \dots, x_n)$.

Действительно, для любого набора $(k_1, \dots, k_n) \in \mathbb{Z}_p^n$ при $(x_1, \dots, x_n)$, равном набору $(k_1, \dots, k_n)$, в этой сумме все слагаемые обращаются в нуль, и только слагаемое $g(k_1, \dots, k_n)f_{k_1, \dots, k_n}(x_1, \dots, x_n)$ равно $g(k_1, \dots, k_n)$, поэтому и вся сумма при $(x_1, \dots, x_n) = (k_1, \dots, k_n)$ равна $g(k_1, \dots, k_n)$. Указанная сумма является многочленом от переменных $x_1, \dots, x_n$ степени не выше $p-1$ по каждой из них. Тем самым существование реализующего функцию $g(x_1, \dots, x_n)$ многочлена доказано.

Для доказательства единственности заметим, что каждый из многочленов от n переменных степени, меньшей p по каждой из них, однозначно определяется набором коэффициентов при своих одночленах $x_1^{k_1} \dots x_n^{k_n}$, $0 \leq k_i \leq p-1$. Этих коэффициентов, как и одночленов, p^n штук, каждый из них независимо от других принимает p значений, поэтому число всех таких многочленов равно p^{p^n} .

Число же различных реализуемых функций тоже равно p^{p^n} , так как каждая из них однозначно определяется набором своих p^n значений при

$$(x_1, \dots, x_n) = (k_1, \dots, k_n), \quad 0 \leq k_i \leq p-1.$$

Поэтому согласно принципу Дирихле каждая из функций реализуется ровно одним многочленом, иначе многочленов не хватило бы для реализации всех функций. $\square$

Используя многочлены над полем $\mathbb{Z}_p$, можно дать другое доказательство теоремы Вильсона: *если p — простое число, то число $(p-1)! + 1$ делится на p .*

Доказательство. Для $p=2$ эту теорему можно проверить непосредственно. Пусть $p > 2$. Согласно малой теореме Ферма многочлен $x^{p-1} - \bar{1}$ над полем $\mathbb{Z}_p$ имеет ровно $p-1$ корень $\bar{1}, \bar{2}, \dots, \overline{p-1}$, поэтому этот многочлен можно разложить на линейные множители

$$x^{p-1} - \bar{1} = (x - \bar{1})(x - \bar{2}) \dots (x - \overline{p-1}).$$

Подставим в полученное тождество $\bar{0}$ и получим, что $-\bar{1} = (-1)^{p-1} \overline{(p-1)!}$, а так как $(p-1)$ — число четное, то $(p-1)! + 1$ делится на p . $\square$

В некоторых случаях более удобной является *интерполяционная формула Ньютона*.

Теорема 72. Для произвольного многочлена $f(x) \in K[x]$ степени n и произвольных $c_0, \dots, c_n \in K$ справедлива формула

$$\hat{f}(x) = a_0 + a_1(x - c_0) + a_2(x - c_0)(x - c_1) + \dots + a_n(x - c_0) \dots (x - c_{n-1}),$$

где $a_i = F_i(c_i)$, $i = 0, \dots, n$, а последовательность функций

$$F_i: \{c_0, \dots, c_{i-2}, c_i, \dots, c_n\} \rightarrow K$$

определяется формулами $F_0(c_i) = f(c_i)$, $i = 0, \dots, n$,

$$F_i(x) = \frac{F_{i-1}(x) - F_{i-1}(c_{i-1})}{x - c_{i-1}}, \quad x \in \{c_0, \dots, c_{i-2}, c_i, \dots, c_n\}.$$

Доказательство. Существование формулы указанного вида можно доказать по индукции, при этом в качестве a_n берется старший коэффициент многочлена $f(x)$.

Единственность коэффициентов a_i также с помощью индукции выводится из формулы

$$\begin{aligned} \hat{f}(c_0) &= a_0; \\ \hat{f}(c_1) &= a_0 + a_1(c_1 - c_0); \\ \hat{f}(c_2) &= a_0 + a_1(c_2 - c_0) + a_2(c_2 - c_0)(c_2 - c_1); \\ &\dots\dots\dots \\ \hat{f}(c_n) &= a_0 + a_1(c_n - c_0) + \dots + a_n(c_n - c_0) \dots (c_n - c_{n-1}), \end{aligned}$$

которые получаются из формулы для $\hat{f}(x)$ подстановками констант c_i , $i = 0, \dots, n$.

Из определения функций F_i , $i = 0, \dots, n$, также по индукции выводятся формулы

$$\begin{aligned} F_0(x) &= a_0 + F_1(x)(x - c_0), \\ F_0(x) &= a_0 + a_1(x - c_0) + F_2(x)(x - c_0)(x - c_1), \\ &\dots\dots\dots \\ F_0(x) &= a_0 + a_1(x - c_0) + \dots + F_n(x)(x - c_0) \dots (x - c_{n-1}). \end{aligned}$$

Подставляя в них константы $c_1, \dots, c_n$ и пользуясь доказанной единственностью коэффициентов a_i , $i = 0, \dots, n$, получаем формулы

$$a_i = F_i(c_i), \quad i = 0, \dots, n. \quad \square$$

Упражнение 61. Проверьте, что вычисление коэффициентов интерполяционного многочлена по формуле Ньютона требует $n^2 + n$ вычитаний, $(n^2 + n)/2$ делений.

Если коэффициенты a_i , $i = 0, \dots, n$, в формуле Ньютона уже вычислены и нам нужно найти значение интерполяционного многочлена

в заданной точке x , то для этого удобно использовать следующую формулу (обобщающую схему Горнера, которая появится у нас дальше)

$$\begin{aligned} f(x) &= a_0 + a_1(x - c_0) + a_2(x - c_0)(x - c_1) + \dots + a_n(x - c_0) \dots (x - c_{n-1}) = \\ &= ((a_n(x - c_{n-1}) + a_{n-1})(x - c_{n-2}) + \dots)(x - c_0) + a_0. \end{aligned}$$

Упражнение 62. Проверьте, что вычисление значения интерполяционного многочлена по этой формуле требует n умножений и $2n$ сложений.

Заметным преимуществом формулы Ньютона при обработке экспериментальных данных является то обстоятельство, что если мы решили добавить еще одну точку в формулу для интерполяции и соответственно увеличить на 1 степень интерполяционного многочлена, то не надо заново пересчитывать все ее коэффициенты, а нужно найти только последний (старший) коэффициент.

Но формула Ньютона не дает явно коэффициентов интерполяционного многочлена, как формула Лагранжа—Варинга.

Задачи и упражнения к § 3.3

Далее рассматриваем только многочлены над полем действительных чисел, если не оговорено противное.

1. Построить многочлен наименьшей степени по таблице значений

x	1	2	3	4
y	2	1	4	3

а) над полем $\mathbb{Q}$; б) над полем $\mathbb{Z}_5$.

2. Пусть $P(x) = \prod_{i=1}^n (x - a_i)$, $l_i(x) = \frac{P(x)}{x - a_i}$. Докажите, что $\sum_{i=1}^n \frac{l_i(x)}{l_i(a_i)} = 1$.

3*. Пусть $P(x) = \prod_{i=1}^n (x - a_i)$. Докажите, что $\sum_{i=1}^n \frac{1}{P'(a_i)} = 0$, при $n > 1$.

4*. Формуле Лагранжа можно придать следующий более элегантный вид

$$\frac{f(x)}{(x - x_1) \dots (x - x_n)} = \sum_{k=1}^n \frac{f(x_k)}{f'(x_k)(x - x_k)},$$

где стоящая слева дробь — правильная.

5. Многочлен $P(x)$ при делении на $x - a$ дает остаток a для всех $a = 1, 2, 3, 4$. Найдите остаток от деления его на $(x - 1)(x - 2)(x - 3)(x - 4)$.

6. Докажите, что если $p(x)$ — многочлен степени n со старшим коэффициентом 1, то при некотором целом $m \in [0, n]$ его модуль не меньше $n!/2^n$.

7. Докажите, что если $p(x)$ — многочлен степени $2n$ и при каждом целом $k \in [-n, n]$ справедливо неравенство $|p(k)| \leq 1$, то при любом $x \in [-n, n]$ справедливо неравенство $|p(x)| \leq 2^{2n}$.

8. Построить многочлен наименьшей степени по таблице значений

а)

x	0	1	2	...	9
y	1	2	4	...	512

; б)

x	1	2	3	...	99
y	1	1/2	1/3	...	1/99

.

9*. Многочлен $p(x)$ степени n удовлетворяет равенству $p(k) = \frac{k}{k+1}$, $k = 0, \dots, n$. Найдите $p(n+1)$.

10*. Многочлен $p(x)$ степени n удовлетворяет равенству $p(k) = \frac{1}{C_{n+1}^k}$, $k = 0, \dots, n$. Найдите $p(n+1)$.

Многочлен называется *целозначным*, если он принимает во всех целых точках только целые значения.

11*. Докажите, что целозначный многочлен имеет вид

$$a_0 + a_1x + \dots + a_n \frac{x(x-1) \dots (x-n+1)}{n!},$$

где $a_i \in \mathbb{Z}$.

У к а з а н и е. Применить формулу Ньютона.

12. Докажите, что операция $\Delta P(x) = P(x+1) - P(x)$ переводит целозначный многочлен в целозначный.

13*. Докажите, что многочлен степени n , принимающий в $n+1$ подряд идущих целых точках только целые значения, является целозначным.

14*. Докажите, что многочлен степени n , принимающий в точках $0, 1, 4, \dots, n^2$ только целые значения, принимает целые значения в любой целой точке вида mt^2 , $t \in \mathbb{Z}$.

15*. Многочлен степени n со старшим коэффициентом 1 при целых значениях аргумента принимает целые значения, делящиеся на m . Докажите, что $m \mid n!$.

16**. Многочлен степени n в любой целой точке равен n -й степени целого числа. Докажите, что он равен n -й степени линейного многочлена с целыми коэффициентами.

§ 3.4. Производные и кратные корни

Рассмотрим кольцо многочленов над произвольным полем F .

Определение 79. *Производной* многочлена

$$f(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$$

называется многочлен $f'(x) = na_0x^{n-1} + (n-1)a_1x^{n-2} + \dots + a_{n-1}$.

Справедливы следующие утверждения о производной многочлена.

Теорема 73.

- (i) Производная многочлена нулевой степени равна 0.
- (ii) Для любого $c \in F$ производная многочлена $x - c$ равна 1.
- (iii) Производная суммы двух многочленов равна сумме производных.
- (iv) Для любых $c \in F$, $f \in F[x]$ справедливо равенство $(cf)' = cf'$, т. е. постоянный множитель можно выносить за знак производной.
- (v) Для любых многочленов $f_1 f_2 \in F[x]$ справедлива формула Лейбница

$$(f_1 f_2)' = f_1' f_2 + f_1 f_2'.$$

- (vi) Для любых многочленов $f_i \in F[x]$, $i = 1, \dots, n$, справедлива обобщенная формула Лейбница

$$(f_1 \dots f_n)' = f_1' f_2 \dots f_n + f_1 f_2' f_3 \dots f_n + \dots + f_1 f_2 \dots f_{n-1}' f_n.$$

- (vii) Для любого многочлена $f \in F[x]$

$$(f^k)' = k f^{k-1} \cdot f'.$$

- (viii) Для любого элемента $c \in F$

$$((x - c)^k)' = k(x - c)^{k-1}.$$

Доказательство. Первые четыре утверждения следуют непосредственно из определения. Формула Лейбница (v) легко доказывается сначала в частном случае, а потом переходим к более общему случаю:

$$(a) \quad f_1(x) = ax^m, \quad f_2(x) = bx^n;$$

$$(б) \quad f_1(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n, \quad f_2(x) = bx^n;$$

$$(в) \quad f_1(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n, \\ f_2(x) = b_0 x^m + b_1 x^{m-1} + \dots + b_{m-1} x + b_m.$$

Утверждение (vi) легко выводится из формулы Лейбница по индукции. Утверждение (vii) является частным случаем предыдущего. Последнее утверждение очевидно следует из предыдущих. $\square$

Естественным образом можно ввести понятие производных высшего порядка.

Определение 80. Производная от первой производной называется *второй производной*, производная от второй производной называется *третьей производной* и т. д.; *n-я производная* — это производная от $(n - 1)$ -й производной. Производная порядка n многочлена f обозначается обычно $f^{(n)}$.

Справедливо следующее обобщение формулы Лейбница.

Теорема 74. Для любых многочленов $f_i \in F[x]$, $i = 1, \dots, n$, и любого натурального k справедливо равенство

$$(f_1 f_2)^{(n)} = \sum_{k=0}^n C_n^k f_1^{(k)} f_2^{(n-k)},$$

где $f^{(0)}$ обозначает f .

Доказательство. Доказательство проводится по индукции. База ($n = 1$) доказана в предыдущей теореме. Шаг индукции обосновывается с помощью предыдущей теоремы и тождества Паскаля (см. с. 48). $\square$

Рассмотрим поле F характеристики 0 и кольцо многочленов над ним.

Определение 81. Элемент $x_0 \in F$ называется *корнем кратности n* многочлена $f(x) \in F[x]$, если $f(x)$ делится без остатка на $(x - x_0)^n$, но не делится на $(x - x_0)^{n+1}$. Корень кратности 1 называется *простым*.

Теорема 75. Элемент $x_0 \in F$ является корнем многочлена $f(x)$ кратности n ($n \geq 2$) тогда и только тогда, когда $f(x_0) = 0$ и он является корнем кратности $n - 1$ у производной многочлена $f'(x)$.

Доказательство. Пусть x_0 — корень кратности n многочлена $f(x)$, тогда по определению $f(x) = (x - x_0)^n \cdot h(x)$, где $h(x)$ не делится на $x - x_0$. Применяя предыдущую теорему, отсюда имеем, что

$$\begin{aligned} f'(x) &= n(x - x_0)^{n-1} \cdot h(x) + (x - x_0)^n \cdot h'(x) = \\ &= (x - x_0)^{n-1} \cdot (n \cdot h(x) + (x - x_0) \cdot h'(x)). \end{aligned}$$

Следовательно, $f'(x)$ делится на $(x - x_0)^{n-1}$, но не делится на $(x - x_0)^n$, так как $h(x)$ не делится на $x - x_0$.

Обратно, пусть $f(x_0) = 0$ и $f'(x)$ делится на $(x - x_0)^{n-1}$. Докажем, что x_0 — корень кратности n многочлена $f(x)$. Предположим, что $f(x) = (x - x_0)^k \cdot h(x)$, где $h(x)$ не делится на $x - x_0$. Тогда

$$\begin{aligned} f'(x) &= k(x - x_0)^{k-1} \cdot h(x) + (x - x_0)^k \cdot h'(x) = \\ &= (x - x_0)^{k-1} \cdot (k \cdot h(x) + (x - x_0) \cdot h'(x)), \end{aligned}$$

многочлен $kh(x) + (x - x_0) \cdot h'(x)$ не делится на $x - x_0$ и, следовательно, x_0 является корнем кратности $k - 1$ производной $f'(x)$, откуда $k = n$. $\square$

Любой многочлен f может быть единственным образом *разложен по степеням* $(x - c)$:

$$f(x) = b_0(x - c)^n + b_1(x - c)^{n-1} + \dots + b_{n-1}(x - c) + b_n$$

Это легко доказывается индукцией по степени многочлена. Действительно, разделим $f(x)$ на $x - c$ с остатком. Получим

$$f(x) = (x - c)f_1(x) + b_n,$$

где b_n — остаток, $f_1(x)$ — многочлен степени $n - 1$. В силу индуктивного предположения

$$f_1(x) = b_0(x - c)^{n-1} + b_1(x - c)^{n-2} + \dots + b_{n-1},$$

откуда $f(x) = b_0(x - c)^n + \dots + b_n$.

Опишем алгоритм для вычисления коэффициентов b_i . Свободный член b_n разложения есть остаток от деления f на $x - c$, b_{n-1} есть остаток при делении неполного частного f_1 на $x - c$, и вычисление последующих коэффициентов требует вычисления неполного частного f_2 при делении f_1 на $x - c$. Далее, b_{n-2} находится как остаток при делении f_2 на $x - c$ и т. д. Красивые формулы для коэффициентов b_i указывает следующая теорема.

Теорема 76 (Тейлор*). *Любой многочлен f степени n можно представить в виде*

$$f(c) + \frac{f'(c)}{1!}(x - c) + \frac{f''(c)}{2!}(x - c)^2 + \dots + \frac{f^{(n)}(c)}{n!}(x - c)^n.$$

Доказательство. Пусть

$$f(x) = d_0 + d_1(x - c) + d_2(x - c)^2 + \dots + d_n(x - c)^n.$$

Продифференцируем k раз обе части этого равенства. Используя правила дифференцирования, получаем, что

$$f^{(k)}(x) = k! d_k + (k + 1)! d_{k+1}(x - c) + \dots + n(n - 1) \dots (n - k + 1) d_n(x - c)^{n-k}.$$

Полагая $x = c$, имеем $f^{(k)}(c) = k! d_k$. □

Задачи и упражнения к § 3.4

1. Определить A и B так, чтобы $(x - 1)^2 \mid Ax^{n+1} + Bx^n + 1$.

2. Докажите, что многочлены

(i) $x^{2n} - nx^{n+1} + nx^n - 1$;

(ii) $x^{2n+1} - (2n + 1)x^{n+1} + (2n + 1)x^n - 1$

имеют один тройной корень.

3. Найдите условие, при котором многочлен $x^5 + ax^3 + b$ имеет двойной ненулевой корень.

* Б. Тейлор (Brook Taylor, 1685–1731) — английский математик, член Лондонского королевского общества.

4. Докажите, что трехчлен $x^n + ax^{n-m} + b$ не может иметь ненулевых корней кратности выше второй.

5. Докажите, что k -членный многочлен $a_1x^{n_1} + \dots + a_kx^{n_k}$ не может иметь ненулевых корней кратности выше $(k-1)$ -й.

6. Докажите, что многочлен $1 + x + x^2/2 + x^3/3! + \dots + x^n/n!$ не имеет кратных корней.

7*. Докажите, что многочлен $1 + x + x^2/2 + x^3/3! + \dots + x^n/n!$ имеет не более одного действительного корня.

8*. Докажите, что многочлен $1 + x + x^2/2 + x^3/3! + \dots + x^n/n!$ не имеет рациональных корней. У к а з а н и е. Применить формулу Лежандра о делимости факториалов.

9. Разложите многочлен $x^6 - 6x^4 - 4x^3 + 9x^2 + 12x + 4$ на множители, не имеющие кратных корней.

10. Если многочлен с целыми коэффициентами принимает в четырех разных целых точках значение a , то он не может принимать ни в одной целой точке значение $a + p$, где p — простое число.

11*. (Эйлер.) Многочлен $n^2 + n + 41$ при $n = 0, 1, \dots, 39$ принимает только простые значения, но при $n = 40$ — нет. Докажите теорему: не существует непостоянного многочлена, принимающего только простые значения при всех натуральных значениях аргумента.

12*. Существует многочлен $f(x)$ n -й степени с целыми коэффициентами такой, что $f(0), \dots, f(n)$ — различные простые числа.

§ 3.5. Схема Горнера*

Деление произвольного многочлена на двучлен может быть выполнено существенно проще, чем деление на произвольный многочлен.

Действительно, если нужно разделить многочлен

$$f(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n \in F[x]$$

на двучлен $x - c$, где $c \in F$, т. е. найти такие $q(x)$ и r , что $q(x) \in F[x]$, $r \in F$, и $f(x) = (x - c)q(x) + r$, естественно искать $q(x)$ в форме $b_0x^{n-1} + b_1x^{n-2} + \dots + b_{n-1}$. Тогда получим равенство

$$\begin{aligned} f(x) &= a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n = \\ &= (x - c)(b_0x^{n-1} + b_1x^{n-2} + \dots + b_{n-1}) + r, \end{aligned}$$

* В. Горнер (William George Horner, 1786–1837) — английский математик.

равносильное цепочке равенств

$$\begin{aligned} a_0 &= b_0, \\ a_1 &= b_1 - cb_0, \\ a_2 &= b_2 - cb_1, \\ &\dots\dots\dots \\ a_{n-1} &= b_{n-1} - cb_{n-2}, \\ a_n &= r - cb_{n-1}, \end{aligned}$$

откуда последовательно определяются коэффициенты $q(x)$ и остаток r :

$$\begin{aligned} b_0 &= a_0, \\ b_1 &= a_1 + cb_0, \\ b_2 &= a_2 + cb_1, \\ &\dots\dots\dots \\ b_{n-1} &= a_{n-1} + cb_{n-2}, \\ r &= a_n + cb_{n-1}. \end{aligned}$$

Заметим, что остаток r равен значению $f(c)$ многочлена $f(x)$ при $x = c$. Действительно, переходя в равенстве $f(x) = (x - c)q(x) + r$ к значениям при $x = c$, получим $f(c) = (c - c)q(c) + r$, откуда $r = f(c)$.

Указанный способ вычисления коэффициентов частного $q(x)$ и остатка r носит название схемы Горнера (хотя она была, по существу, известна, например, и Ньютону, и Руффини, и даже в Китае в XIII в.).

Далее *сложностью алгоритма* будем называть число выполняемых в нем арифметических операций.

В приведенном выше алгоритме Горнера использовались только операции сложения-вычитания и умножения и фактически была доказана следующая

Теорема 77. *Частное и остаток от деления многочлена $f(x)$ степени n на $x - c$ находятся со сложностью n плюс число ненулевых коэффициентов y многочлена $f(x)$ минус единица.*

Упражнение 63. Найдите неполное частное и остаток при делении многочлена x^5 на $x - 2$.

Выпишем последовательно коэффициенты многочлена x^5 и, после вертикальной черты, число 2:

$$1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad | \quad 2.$$

Под этой строкой запишем коэффициенты неполного частного и остаток, пользуясь только что выведенными формулами:

$$\begin{array}{cccccc|c} 1 & 0 & 0 & 0 & 0 & 0 & 2 \\ 1 & 2 & 4 & 8 & 16 & \underline{32} & \end{array}$$

(остаток — подчеркнутое число). Итак,

$$x^5 = (x - 2)(x^4 + 2x^3 + 4x^2 + 8x + 16) + 32.$$

З а м е ч а н и е. В связи с этим примером отметим, что деление x^{100} на $x - 1000$ на компьютере таким способом выполнить затруднительно, потому что остаток будет равен 10^{30} и вызовет переполнение. Не все, что легко в теории, является таким и на практике.

Описанному в предыдущем параграфе алгоритму разложения многочлена по степеням двучлена $x - c$ можно придать следующий вид.

Теорема 78. Младшие $k + 1$ коэффициентов многочлена $f(x + c)$, равные

$$f(c), f'(c), \dots, f^{(k)}(c)/k!,$$

можно вычислить со сложностью $(k + 1)(2n - k)$, где $n = \deg f(x)$. В частности, все коэффициенты вычисляются со сложностью $n(n + 1)$.

Д о к а з а т е л ь с т в о. Обозначим $G(n, k + 1)$ сложность этого вычисления. С помощью схемы Горнера со сложностью $2n$ вычислим $q(x)$ и $f(c)$, где

$$\tilde{f}(x) = (x - c)q(x) + f(c).$$

Тогда

$$f(x + c) = xq(x + c) + p(c),$$

и для вычисления остальных k коэффициентов достаточно найти k младших коэффициентов у многочлена $q(x + c)$ степени $n - 1$. Поэтому

$$G(n, k + 1) \leq G(n - 1, k) + 2n, \quad G(n, 1) \leq 2n,$$

значит,

$$G(n, k + 1) \leq 2n + 2(n - 1) + \dots + 2(n - k) = (k + 1)(2n - k).$$

При $k = n$ получаем $G(n, n + 1) = n(n + 1)$, причем используется $n(n + 1)/2$ сложений и столько же умножений на константу c .

Тот факт, что коэффициент при x^k в многочлене $f(x + c)$ равен $f^{(k)}(c)/k!$, следует из формулы Тейлора. $\square$

З а м е ч а н и е. Если $c = 1$, то реально умножений вообще не производится. В общем случае почти все умножения можно сэкономить, если предварительно вычислить $c^2, \dots, c^n$, и от многочлена

$$\tilde{f}(x) = a_0 + \dots + a_n x^n$$

перейти к многочлену

$$F(x) = \tilde{f}(xc) = a_0 + \dots + a_n c^n x^n,$$

вычислив его коэффициенты $a_0, a_1 c, \dots, a_n c^n$, далее получить разложение $F(x)$ по степеням $x - 1$

$$F(x) = b_0 + b_1(x - 1) + \dots + b_n(x - 1)^n$$

с помощью $n(n+1)/2$ сложений, откуда при $y = xc$

$$f(y) = b_0 + b_1(y/c - 1) + \dots + b_n(y/c - 1)^n = b_0 + \frac{b_1}{c}(y - c) + \dots + \frac{b_n}{c^n}(y - c)^n,$$

значит, нужные нам коэффициенты $f^{(k)}(c)/k!$ находятся по формулам b_k/c^k с помощью n делений.

Упражнение 64. Разложим многочлен x^5 по степеням $x - 2$. Применяя схему Горнера, получим:

$$\begin{array}{r|rrrrrr} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 4 & 8 & 16 & \underline{32} \\ 1 & 4 & 12 & 32 & \underline{80} & \\ 1 & 6 & 24 & \underline{80} & & \\ 1 & 8 & \underline{40} & & & \\ 1 & \underline{10} & & & & \\ 1 & & & & & \end{array}$$

где остатки подчеркнуты. Таким образом,

$$x^5 = (x - 2)^5 + 10(x - 2)^4 + 40(x - 2)^3 + 80(x - 2)^2 + 80(x - 2) + 32.$$

Для приближенного вычисления корней многочлена бывает нужно найти одновременно $f(c)$ и $f'(c)$. Выполнить это можно при помощи схемы Горнера, вычислив два коэффициента разложения f по степеням $x - c$.

Упражнение 65. Для многочлена $x^3 - x - 1$ вычислим $f(1,2)$ и $f'(1,2)$. Применим схему Горнера:

$$\begin{array}{r|rrrr} 1 & 0 & -1 & -1 & \\ 1 & 1,2 & 0,44 & \underline{-0,472} & \\ 1 & 2,4 & \underline{3,32} & & \end{array}$$

Итак, $f(1,2) = -0,472$ и $f'(1,2) = 3,32$.

В качестве еще одного применения схемы Горнера опишем *алгоритм перевода из двоичной системы в десятичную* и обратно.

Сначала переведем число из двоичной системы в восьмеричную. Для этого разбиваем справа налево его цифры на тройки (последняя тройка на самом деле может быть парой или одной цифрой) и переводим их в восьмеричную систему схемой Горнера (выполняемой устно). Например,

$$(1111110000)_2 = (1.111.110.000)_2 = (1760)_8.$$

Выполним перевод из восьмеричной системы в десятичную. Пусть число $u = (u_n \dots u_1)_8$. На k -м шаге выполняем над полученной на предыдущем шаге записью в десятичной арифметике действия

$$\overline{u_n \dots u_{n-k-1}} - 2 \cdot \overline{u_n \dots u_{n-k}} = \overline{v_{n+1} \dots v_{n-k-1}}$$

и получаем запись

$$\overline{v_{n+1} \dots v_{n-k-1}.u_{n-k-2} \dots u_1},$$

где точка используется вместо десятичной запятой, а старшие разряды могут оказаться нулевыми и в реальных вычислениях участвовать не будут. На $(n-1)$ -м шаге получаем десятичную запись числа u . Например, $(1760)_8 = (1008)_{10}$:

$$\begin{array}{r} \underline{-(1.7\ 6\ 0)_8} \\ 2 \\ \hline 1\ 5.6\ 0 \\ \underline{-\ 3\ 0} \\ 1\ 2\ 6.0 \\ \underline{-\ 2\ 5\ 2} \\ (1\ 0\ 0\ 8)_{10} \end{array}$$

Алгоритм перевода из десятичной системы в двоичную почти такой же. Сначала переводим в восьмеричную запись. Для этого, пользуясь восьмеричной арифметикой, на k -м шаге выполняем над полученной на предыдущем шаге записью действия:

$$\overline{u_n \dots u_{n-k-1}} + 2 \cdot \overline{u_n \dots u_{n-k}} = \overline{v_{n+1} \dots v_{n-k-1}}$$

и получаем запись

$$\overline{v_{n+1} \dots v_{n-k-1}.u_{n-k-2} \dots u_1}$$

(поначалу $(n+1)$ -е разряды окажутся нулевыми и в реальных вычислениях участвовать не будут). На $(n-1)$ -м шаге получаем восьмеричную запись числа u . Например, $(1945)_{10} = (3631)_8$:

$$\begin{array}{r} \underline{+(1.9\ 4\ 5)_{10}} \\ 2 \\ \hline 2\ 3.4\ 5 \\ \underline{+\ 4\ 6} \\ 3\ 0\ 2.5 \\ \underline{+\ 6\ 0\ 4} \\ (3\ 6\ 3\ 1)_8 \end{array}$$

Здесь числа левее точки записаны в восьмеричной системе. Далее переводим восьмеричное n -значное число в двоичное (вычисляя для каждой восьмеричной цифры двумя делениями на два с остатком ее двоичную запись).

Задачи и упражнения к § 3.5

1. Укажите ускоренный вариант схемы Горнера, удобный для вычисления четных и нечетных многочленов, и дайте оценку его сложности.
2. Переведите из десятичной в двоичную число 12345678987654321.
3. Переведите из двоичной в десятичную число 10101010101010101.
4. Дайте подробное обоснование изложенных в этом параграфе алгоритмов перевода из двоичной в десятичную систему и обратно.
5. На одной из шумерских клинописных табличек написано число $60^8 + 10 \cdot 60^7$. Переведите его из шестидесятеричной системы в десятичную.
- 6*. (Параллельная схема Горнера.) Если компьютер имеет k параллельно работающих процессоров, операции обмена между которыми занимают пренебрежимо малое время, то вычисление значения многочлена степени n в заданной точке требует не более

$$2n/k + \max_{j \leq k} l(j) + \log_2 k + O(1)$$

единиц времени, где $l(m)$ — время вычисления x^m .

У к а з а н и е. Положим $n = mk + s$, $0 \leq s < k$, и представим $p(x)$ в виде

$$\sum_{j=0}^{k-1} x^j p_j(x^k) = \sum_{j=0}^s x^j \sum_{i=0}^m u_{ki+j} x^{ki} + \sum_{j=s+1}^{k-1} x^j \sum_{i=0}^{m-1} u_{ki+j} x^{ki}.$$

На j -м процессоре вычисляем $x^j p_j(x^k)$. Для этого на $(k-1)$ -м процессоре вычисляется со сложностью $l(k) + O(1)$ степени x^{k-1} и x^k и последняя передается на остальные процессоры, которые тем временем вычисляют степени x^j . После этого все процессоры вычисляют $x^j p_j(x^k)$ со сложностью $2n/k + O(1)$ каждый (используя обычную схему Горнера).

Остается сложить полученные результаты за время $\log_2 k + O(1)$, используя параллельно $k/2$ процессоров.

7*. Для одновременного вычисления значений многочлена в нескольких точках схему Горнера иногда можно немного ускорить.

Докажите, что для одновременного вычисления значений $p(c)$ и $p(-c)$ достаточно $2n + 1$ операции, где n — степень многочлена $p(x)$.

У к а з а н и е. Разделим $p(x)$ на $x^2 - c^2$. Получим равенство

$$p(x) = q(x)(x^2 - c^2) + r_1 x + r_0.$$

Представляя $p(x)$ в виде суммы многочленов, содержащих только четные и только нечетные степени переменной, получим, что $p(x) = p_0(x^2) + x p_1(x^2)$, где сумма степеней многочленов $p_0(x)$ и $p_1(x)$ равна $n - 1$.

Деля их на $x - c^2$, имеем

$$p_0(x) = q_0(x)(x - c^2) + k_0, \quad p_1(x) = q_1(x)(x - c^2) + k_1.$$

Отсюда

$$\begin{aligned} q(x)(x^2 - c^2) + r_1x + r_0 &= p(x) = p_0(x^2) + xp_1(x^2) = \\ &= q_0(x^2)(x^2 - c^2) + k_0 + x(q_1(x^2)(x^2 - c^2) + k_1) = \\ &= (x^2 - c^2)(q_0(x^2) + xq_1(x^2)) + k_1x + k_0, \end{aligned}$$

значит,

$$r_1 = k_1, \quad r_0 = k_0, \quad q(x) = q_0(x^2) + xq_1(x^2).$$

Сложность деления на $x^2 - c^2$ не превосходит $2n - 2$. Для вычисления

$$p(c) = q(c)(c^2 - c^2) + rc + r = rc + r,$$

$$p(-c) = q(-c)(c^2 - c^2) + r_1(-c) + r_0 = -r_1c + r_0$$

нужно дополнительно 3 операции.

§ 3.6. Аддитивные цепочки

Назовем *аддитивной цепочкой* любую начинающуюся с 1 последовательность натуральных чисел $a_0 = 1, a_1, \dots, a_m$, в которой каждое число является *суммой каких-то двух предыдущих чисел* (или *удвоением* какого-то предыдущего числа). Обозначим $l(n)$ *наименьшую длину* аддитивной цепочки, заканчивающейся числом n . Для определенности под длиной цепочки $a_0 = 1, a_1, \dots, a_m$ понимаем число m .

Пр и м е р ы. 1. Последовательность 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14 — аддитивная цепочка.

2. Последовательность 1, 2, 3, 5, 7, 14 — минимальная цепочка для 14, т. е. $l(14) = 5$.

3. Аддитивные цепочки можно изображать в виде ориентированного графа, в котором в вершину a_i идут ребра от вершин a_j, a_k , если $a_i = a_j + a_k$ (в случае, если такое представление неоднозначно, выбираем любое из них и рисуем только два ребра). Если из какой-то вершины выходит только одно ребро, то для краткости можно «склеить» эту вершину с той вершиной, в которую ведет это ребро. Граф для предыдущего примера см. рис. 21.

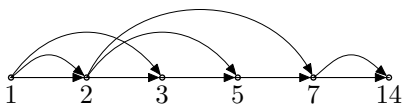


Рис. 21

Можно считать, что все числа в цепочке *разные*, так как этого легко достичь, просто удаляя из нее повторяющиеся числа и располагая числа в цепочке в порядке возрастания.

Упражнение 66. Докажите, что наименьшее число операций умножения, требующихся для возведения числа x в степень n , равно $l(n)$.

Таким образом, вычисление x^{14} требует не 13 умножений, а только 5.

Обозначим $\lambda(n) = \lfloor \log_2 n \rfloor$ *уменьшенную на единицу длину* двоичной записи числа n , а $\nu(n)$ — *сумму цифр* (другими словами, число единиц) в ней.

Примеры. 1. При $n = 14$, очевидно, $\lambda(14) = 3$.

2. Так как $14 = (1110)_2$, то $\nu(14) = 3$.

Записывая число n в двоичной системе и используя схему Горнера, можно написать аддитивную цепочку для числа n длины $\lambda(n) + \nu(n) - 1$ следующим образом

$$\begin{aligned} n &= 2^m b_m + \dots + b_0 = (\dots (2b_m + b_{m-1})2 + \dots + b_1)2 + b_0, \\ a_0 &= b_m = 1, \quad a_1 = 2a_0 = 2, \quad a_2 = a_1 + b_{m-1}, \quad a_3 = 2a_2, \dots, \\ a_{2m-1} &= 2a_{2m-2}, \quad a_{2m} = a_{2m-1} + b_0, \end{aligned}$$

где число удвоений равно $m = \lambda(n)$, а число прибавлений единицы равно $\nu(n) - 1$.

Примеры. 1. Так как $14 = (1110)_2 = 2^3 + 2^2 + 2 = ((1 \cdot 2 + 1) \cdot 2 + 1) \cdot 2$, то получается цепочка 1, 2, 3, 6, 7, 14.

2. Этой цепочке соответствует такой алгоритм возведения в степень:

$$x, \quad x^2, \quad x^3 = x^2 \cdot x, \quad x^6 = (x^3)^2, \quad x^7 = x^6 \cdot x, \quad x^{14} = (x^7)^2.$$

3. Для запоминания последовательности операций в случае ее многократного исполнения можно заменить в двоичной записи показателя степени $14 = (1110)_2$ каждую единицу, начиная слева (со старших разрядов), кроме самой первой, на слог КУ, а каждый нуль — на букву К, тогда получим слово КУКУК, в котором буквы К означают возведение в квадрат, а буквы У — умножение на основание степени.

Тем самым доказана

Теорема 79 (бинарный метод). *Справедливо неравенство*

$$l(n) \leq \lambda(n) + \nu(n) - 1.$$

Интересно, что бинарный метод был фактически известен древним индусам, а задача о нахождении функции $l(n)$ появилась в одном французском журнале в 1894 г.

Поэтому

$$l(n) < (2^{k-1} + 1) + (m + 2 + s - k) < m + 2 + \left\lceil \frac{m+1}{k} \right\rceil + 2^{k-1} - k.$$

Можно считать, что $n \neq 2^m$, тогда $m + 1 = \lceil \log_2 n \rceil$ и

$$l(n) < \lceil \log_2 n \rceil (1 + 1/k) + 2^{k-1} - k + 2. \quad \square$$

Следствие из теоремы 80.

$$\lim_{n \rightarrow \infty} l(n) / \log_2 n = 1.$$

Доказательство. Применяем доказанную теорему при

$$k = \lambda(\lambda(n)) - 2\lambda(\lambda(\lambda(n))). \quad \square$$

Если нужно быстро вычислить сразу несколько степеней, то можно построить *дерево степеней* таким образом. *Корнем* дерева является 1, единственная вершина первого уровня, из нее выходит ребро в вершину 2 второго уровня, и когда дерево уже построено до k -го уровня, то, выбрав любое число n из этого уровня и выписав все числа $a_1 = 1, a_2, \dots, a_k = n$, лежащие на пути из корня до вершины n , соединяем эту вершину с вершинами $n + a_1, \dots, n + a_k$, которые помещаем на $(k + 1)$ -м уровне. В процессе построения повторно одинаковые вершины в дерево, естественно, не заносятся. Эта процедура называется методом дерева степеней.

Задачи и упражнения к § 3.6

1. Докажите, что $\nu(n)$ можно рекуррентно определить следующим образом

$$\nu(1) = 1, \quad \nu(2n) = \nu(n), \quad \nu(2n + 1) = \nu(n) + 1,$$

а функцию $\lambda(n)$ можно рекуррентно определить следующим образом

$$\lambda(1) = 0, \quad \lambda(2n) = \lambda(2n + 1) = \lambda(n) + 1.$$

2. Докажите, что если аддитивная цепочка для числа n имеет длину m , то $n \leq 2^m$.

3. Докажите неравенство $l(n) \geq \log_2 n$ и приведите примеры, когда оно обращается в равенство.

4. Докажите, что если в аддитивной цепочке для числа n имеется k удвоений и m неудвоений, то $n \leq 2^{k-1} F_{m+3}$, где F_l — последовательность Фибоначчи.

5. Докажите неравенство $l(n) \leq 2 \log_2 n$.

6*. Докажите неравенство $l(nm) \leq l(n) + l(m) - 1$ (метод множителей).

7*. Докажите следствие из теоремы Брауэра с оценкой

$$\log_2 n \left(1 + \frac{1}{\log_2 \log_2 n} + \frac{C \log_2 \log_2 \log_2 n}{(\log_2 \log_2 n)^2} \right),$$

где $C > 0$ — некоторая константа.

8*. Покажите, приведя примеры, что иногда метод множителей лучше, чем бинарный метод, а иногда наоборот. Покажите, что такие примеры встречаются бесконечно часто.

9*. Покажите, приведя примеры, что метод дерева степеней бывает лучше метода множителей и бинарного метода.

10*. Для быстрого вычисления больших чисел Фибоначчи можно использовать следующий прием. Если уже вычислена пара чисел (F_k, F_{k-1}) , то пару (F_k, F_{k+1}) находим одним сложением, а пару

$$(F_{2k}, F_{2k-1}) = (F_k^2 + 2F_k F_{k-1}, F_k^2 + F_{k-1}^2)$$

находим еще 6 операциями и применяем бинарный метод.

Докажите, что сложность вычисления F_n не превосходит $C \log_2 n$.

11*. Покажите, что многочлен $p_n(x) = 1 + x + \dots + x^{n-1}$ можно вычислить с помощью $l(n)$ умножений, одного вычитания и одного деления.

12*. Покажите, что многочлен $p_n(x)$ можно вычислить с помощью $2l(n) - 2$ умножений и $l(n)$ сложений.

У к а з а н и е. Если $x^m = x^k x^j$ — очередной шаг минимальной цепочки для вычисления x^n , то делаем шаг $p_m = p_k x^j + p_j$.

13. Проверьте тождество $p_{2^n}(x) = (x^{2^{n-1}} + 1)(x^{2^{n-2}} + 1) \dots (x + 1)$.

14*. Покажите, что $l(2^n - 1) \leq n + 2 \log_2 n$.

Гипотеза Шольца о том, что $l(2^n - 1) \leq n + l(n) - 1$, до сих пор не доказана.

15. Можно обобщить понятие аддитивных цепочек, добавив операцию вычитания. Докажите, что для таких цепочек $l(2^n - 1) \leq n + 1$. Выполняется ли здесь равенство?

Доказано, однако, что при использовании вычитания все равно для почти всех n нижняя оценка для $l(n)$ имеет вид

$$l(n) \geq \log_2 n \left(1 + \frac{1 - \varepsilon_n}{\log_2 \log_2 n} \right),$$

где ε_n стремится к нулю.

16*. Покажите, как с помощью бинарного метода можно на простейшем калькуляторе с операцией $\sqrt{}$, но без операции возведения в степень, приближенно вычислять функцию x^y , где y — двоично-рациональное число.

В следующих задачах без аддитивных цепочек вполне можно обойтись.

17. Найдите последнюю цифру числа 7^{7^7} .

18*. Найдите подстановку

$$\begin{pmatrix} 123456789 \\ 451236897 \end{pmatrix}^{10^{10}}.$$

А в следующей задаче без бинарного метода возникнут трудности.

19*. Найдите $10^{10^{10}} \bmod 1999$.

§ 3.7. Приближенное вычисление корней многочленов

Здесь мы кратко опишем некоторые методы приближенного вычисления корней уравнений. Их полезно знать и уметь применять, но знать доказательства совсем не обязательно, тем более что они скорее относятся к анализу, а не алгебре.

Простейший и наиболее старый метод вычисления называется иногда «цифра за цифрой». В применении к вычислению квадратных корней он был открыт еще в Древней Индии. Для приближенного поиска корней произвольных алгебраических уравнений его первым применил Виет. Одной из вариаций этого метода является так называемый «метод вилки», названный так артиллеристами. Идея его такова: если при некотором угле наклона орудия зафиксирован недолет, а при большем угле — перелет, то следующий угол наклона выбирают как среднее арифметическое двух этих углов.

В применении к поиску корней уравнения $f(x) = 0$ на отрезке $[a, b]$ это выглядит следующим образом. Положим $x_0 = a$, $y_0 = b$, и если на n -м шаге вычисления мы нашли приближения x_n, y_n такие, что $f(x_n)f(y_n) < 0$, то вычисляем $z_n = (x_n + y_n)/2$, $f(z_n)$, и в случае $f(z_n)f(x_n) < 0$ полагаем $x_{n+1} = x_n$, $y_{n+1} = z_n$, а в случае $f(z_n)f(y_n) < 0$ полагаем $x_{n+1} = z_n$, $y_{n+1} = y_n$.

Очевидно, что таким путем можно найти все простые корни любого многочлена с любой заданной точностью. Этот метод хорош еще тем, что пригоден для поиска корней у любой непрерывной функции, даже в условиях, когда нам про нее ничего не известно, но по нашему требованию вычисляют любые ее значения. В таких условиях этот метод может считаться оптимальным.

Если начальные значения x_0, y_0 целые, то указанный метод находит разложение корня в двоичную дробь. Если мы хотим найти десятичное приближение, надо каждый отрезок $[x_n, y_n]$ разбивать на 10 равных частей и искать x_{n+1}, y_{n+1} такими, что $y_{n+1} - x_{n+1} = (y_n - x_n)/10$. Иногда

для поиска очередного приближения вместо уравнения $f(x) = 0$ на отрезке $[x_n, y_n]$ рассматривают уравнение $g(y) = 0$, $g(y) = f(x_n + (y_n - x_n)y/10)$ на отрезке $[0, 10]$, и так можно делать на каждом шаге вычисления. При этом мы избавляемся от дробей, но сталкиваемся с быстрым ростом коэффициентов у последовательности уравнений.

Для ускорения работы нет необходимости вычислять при этом все 11 значений $g(0), \dots, g(10)$, так как можно, применив метод вилки, сделать это за 3 или 4 вычисления значений $g(y)$.

В этом методе для вычисления $f(x_n)$ применяется схема Горнера. Ее использование вдохнуло новую жизнь в этот метод, почему его стали даже иногда называть *методом Горнера* *.

Самым эффективным методом приближенного вычисления корней является *метод Ньютона*. К достоинствам этого метода относится то, что он применим не только к многочленам, но и к любым дифференцируемым функциям, и то, что он допускает широкие обобщения, например, с его помощью можно решать системы уравнений, в том числе и в комплексных числах. Идея, на которой он основан, имеет также важные приложения, но мы не будем здесь их рассматривать, а ограничимся только решением алгебраических уравнений.

Другим его достоинством является очень быстрая сходимость.

Третье его достоинство — то, что он является *итерационным* методом, а эти методы устойчивы относительно ошибок вычислений: если очередная итерация выполнена с ошибкой, то довольно часто это не приводит к ошибке в ответе.

Ньютонова итерация делается следующим образом: если x_n — полученное приближение к корню уравнения $f(x) = 0$, то новое приближение находится по формуле **

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)},$$

где $f'(x_n)$ — производная функции f в точке x_n . Геометрический смысл этой формулы таков: нужно через точку $(x_n, f(x_n))$ графика функции $y = f(x)$ провести касательную, тогда она пересекает ось Ox в точке x_{n+1} .

Упражнение 67. Докажите предыдущее утверждение.

* До Горнера объем вычислений при использовании этого метода был настолько велик, что один из математиков XVII в. назвал приближенное вычисление корней уравнений работой, недостойной христианина.

** Сама эта формула принадлежит Рафсону и в Англии известна как формула Ньютона—Рафсона.

С помощью метода Ньютона очень быстро вычисляются квадратные корни и корни более высокой степени.

Примеры. 1. Для квадратного корня $\sqrt{N}$ ньютонова итерация* имеет вид

$$x_{n+1} = \frac{1}{2} \left(x_n + \frac{N}{x_n} \right).$$

2. Для корня m -й степени $\sqrt[m]{N}$ ньютонова итерация имеет вид

$$x_{n+1} = \frac{1}{m} \left((m-1)x_n + \frac{N}{x_n^{m-1}} \right).$$

Упражнение 68. Покажите, что это действительно ньютоновы итерации в применении к уравнению $x^m - N = 0$, $N > 0$.

Можно доказать, что они будут почти всегда сходиться к корню независимо от выбора начального значения x_0 . Для квадратного корня это можно сделать совсем элементарно.

Упражнение 69. 1. Докажите для ньютоновых приближений к $\sqrt{N}$ тождество

$$\frac{x_n - \sqrt{N}}{x_n + \sqrt{N}} = \left(\frac{x_0 - \sqrt{N}}{x_0 + \sqrt{N}} \right)^{2^n}.$$

2. Докажите, что если $\left| \frac{x_n - \sqrt{N}}{x_n + \sqrt{N}} \right| < 1$, то $\lim_{n \rightarrow \infty} x_n = \sqrt{N}$, а если $\left| \frac{x_n - \sqrt{N}}{x_n + \sqrt{N}} \right| > 1$, то $\lim_{n \rightarrow \infty} x_n = -\sqrt{N}$.

Однако для ускорения вычислений лучше взять x_0 как можно ближе к корню. Например, если $1/2 \leq N < 1$, то простейшее наилучшее приближение есть $0,5903N + 0,4173$. После этого уже две итерации дают 9 десятичных знаков после запятой.

Упражнение 70. Проверьте это.

Если $0,1 \leq N \leq 10$, то в качестве приближения с точностью $1/12$ можно взять $(1 + 4N)/(4 + N)$.

В общем случае неизвестны удобные необходимые и достаточные условия сходимости метода Ньютона при данной начальной точке x_0 . Приведем без доказательства некоторые достаточные условия его сходимости.

Теорема 81 (Фурье).** Пусть функция $f(x)$ определена на отрезке $[a, b]$, на его концах имеет разные знаки (т.е. $f(a)f(b) < 0$),

* Кажется, известная еще древнегреческому математику Герону Александрийскому.

** Ж. Фурье (Jean Baptiste Joseph Fourier, 1768–1830) — знаменитый французский математик. Участник Египетской экспедиции Наполеона.

имеет на нем единственный корень и две производные, причем везде $f'(x)f''(x) \neq 0$, и $f(a)f''(a) > 0$. Тогда при $x_0 = a$ ньютоновы итерации x_n сходятся к корню, причем если выполнить еще итерации по формуле

$$y_{n+1} = y_n - f(y_n)/f'(x_n), \quad y_0 = b$$

(похожей на ньютоновы итерации, но вместо y_n в одном месте используется x_n), то y_n тоже будет сходиться к корню, но с другой стороны. Если $f''(x)$ непрерывна на отрезке $[a, b]$, то

$$\lim_{n \rightarrow \infty} \frac{|y_{n+1} - x_{n+1}|}{(y_n - x_n)^2} = \frac{1}{2} \left| \frac{f''(c)}{f'(c)} \right|,$$

где c — искомый корень.

З а м е ч а н и е. Словами доказанную формулу формулируют так: расстояние между x_n и y_n убывает по квадратичному закону. Это очень быстро, гораздо быстрее, чем в методе вилки. Но последовательность y_n дает гораздо худшее приближение к корню, чем x_n , а именно, доказано, что

$$\lim_{n \rightarrow \infty} \left| \frac{y_n - c}{x_n - c} \right| = +\infty.$$

Поэтому в качестве приближения берут x_n , а y_n используют только для контроля достигнутой точности (иногда можно обойтись и без вычисления y_n).

Для ускорения сходимости последовательности y_n Данделен* предложил использовать итерации

$$y_{n+1} = y_n - f(y_n) \frac{y_n - x_n}{f(y_n) - f(x_n)}.$$

Вычислять их немного сложнее, но зато справедлива

Теорема 82 (Данделен). Если выполнены условия Фурье, то

$$\lim_{n \rightarrow \infty} \left| \frac{y_n - c}{x_n - c} \right| = g(y_0),$$

где g — некоторая монотонная функция, причем

$$\lim_{|y_0 - x_0| \rightarrow 0} g(y_0) = 0.$$

В качестве ответа обычно берут среднее арифметическое x_n и y_n при последней итерации. При решении алгебраических уравнений для вычисления значений $f(x)$ используют схему Горнера.

* Ж. Данделен (Germinal Pierre Dandelin, 1794–1847) — бельгийский математик и инженер.

З а м е ч а н и е. При всех его достоинствах метод Ньютона довольно капризен, он может и не сходиться, и пользоваться им нужно уметь.

В случае, если уравнение дано в виде $f(x) = x$ (а к этому виду можно привести любое уравнение), можно для его решения использовать простейший *итерационный процесс*: $x_{n+1} = f(x_n)$. Очевидно, что если y — корень уравнения, то при $x_0 = y$ последовательность стабильна: $x_n = y$.

Если $f(a) > a$, $a < b$, $f(b) < b$, функция $f(x)$ непрерывна, монотонно возрастает, и уравнение $f(x) = x$ имеет ровно один корень на отрезке $[a, b]$, то последовательность $x_{n+1} = f(x_n)$ при любом начальном значении сходится к этому корню.

Действительно, если, например, x_0 таково, что $f(x_0) > x_0$, то последовательность $x_{n+1} = f(x_n)$ монотонно возрастает, ограничена (почему?) и поэтому имеет предел, который в силу непрерывности совпадает с корнем.

Можно доказать, что если в окрестности корня производная функции по модулю меньше единицы, то в этой окрестности указанная последовательность сходится к корню.

Однако, если, например, в окрестности корня выполняется неравенство $|f'(x)| > 1$, то эта последовательность удаляется от корня.

П р и м е р ы. 1. Если $x_{n+1} = \sin x_n$, $x_0 = 1$, то $x_n \rightarrow 0$.

2. Если $x_{n+1} = \operatorname{tg} x_n$, $x_0 = 1$, то x_n не стремится к нулю.

Если уравнение не имеет вида $f(x) = x$, то его можно привести к этому виду по-разному. Иногда после этого метод итераций дает ответ, иногда нет.

П р и м е р ы. 1. Если уравнение $x^2 = x + 1$, положительный корень которого $(1 + \sqrt{5})/2$ является так называемым золотым сечением, переписать в виде $x^2 - 1 = x$, то итерационная последовательность $x_{n+1} = x_n^2 - 1$ будет либо расходиться, либо закидываться, так как четная функция $f(x) = x^2 - 1$, убывая, переводит отрезок $[-1, 0]$ в себя, меняя местами его концы, поэтому четный многочлен $f_n(x) = f(f_{n-1}(x))$ при четном n будет, возрастая, отображать этот отрезок в себя, а при нечетном n будет, убывая, отображать этот отрезок в себя, и в первом случае уравнение $f_n(x) = x$ имеет на нем корни 0 , $(1 - \sqrt{5})/2$, -1 , а во втором случае — один корень внутри отрезка, которым может быть только $(1 - \sqrt{5})/2$. На отрезке $[0, 1]$ корней нет, а вне отрезка есть только корень $(1 + \sqrt{5})/2$.

2. Если уравнение $x^2 = x + 1$ переписать в виде $x = 1 + 1/x$, то итерационная последовательность $x_{n+1} = 1 + 1/x_n$ при $x_0 > 0$ будет сходиться к корню $(1 + \sqrt{5})/2$. Если возьмем $x_0 = 1$, то полученная последовательность совпадет с уже знакомым нам разложением золотого сечения в цепную дробь.

3. Если уравнение $x^2 = x + 1$ переписать в виде $x = \sqrt{1+x}$, то итерационная последовательность $x_{n+1} = \sqrt{1+x_n}$ при $x_0 > 0$ будет сходиться к корню $(1 + \sqrt{5})/2$. Если возьмем $x_0 = 1$, то получим красивую, но бесполезную с вычислительной точки зрения формулу

$$\frac{1 + \sqrt{5}}{2} = \sqrt{1 + \sqrt{1 + \sqrt{1 + \sqrt{1 + \dots}}}}$$

Итерационные последовательности вида $f_n(x) = f(f_{n-1}(x))$, в особенности не сходящиеся и закликивающиеся, вызывают в настоящее время большой интерес. Их исследование нетривиально даже в случае квадратного трехчлена.

Рассмотрим простой пример. Пусть $f(x) = 2x^2 - 1$, тогда $f_n(x)$ — четный многочлен степени 2^n , совпадающий с *многочленом Чебышёва* * $T_{2^n}(x)$. Этот многочлен переводит отрезок $[-1, 1]$ в себя, пробегая его 2^n раз, точнее, его можно разбить на 2^n отрезков монотонности, каждый из которых отображается на отрезок $[-1, 1]$, многочлен имеет 2^n корней на этом отрезке и на единицу больше чередующихся экстремумов.

Упражнение 71. Докажите это.

Впрочем, то же самое верно и для многочлена Чебышёва любой степени.

Из приведенных фактов следует, что уравнение $f_n(x) = x$ имеет 2^n корней.

Любой корень y уравнения $f_n(x) = x$, не являющийся корнем подобных уравнений меньшей степени, порождает итерационную последовательность периода n .

Упражнение 72. 1. Докажите предыдущее утверждение.

2. Используя формулу $T_n(x) = \cos(n \arccos x)$ и применяя тригонометрию, найдите все корни уравнения $T_n(x) = x$.

Использование идеи итерации позволяет иногда решать не только нетривиальные уравнения, но и системы, например, система

$$\begin{cases} f(x_1) = x_2; \\ f(x_2) = x_3; \\ f(x_3) = x_1 \end{cases}$$

сводится к уравнению $f_3(x) = f(f(f(x))) = x$.

* Общее определение этих многочленов будет дано в §4.17.

Метод итераций можно применить к решению систем и другим способом. Например, если имеем систему

$$\begin{cases} x_1 = f_1(x_1, x_2); \\ x_2 = f_2(x_1, x_2), \end{cases}$$

где отображение $F(x_1, x_2) = (f_1, f_2)$ отображает прямоугольник в себя,

$$F: [a_1, b_1] \times [a_2, b_2] \rightarrow [a_1, b_1] \times [a_2, b_2],$$

причем всегда выполняется неравенство

$$|f_1(x_1, x_2) - f_1(y_1, y_2)| + |f_2(x_1, x_2) - f_2(y_1, y_2)| < |x_1 - y_1| + |x_2 - y_2|,$$

то метод итераций, начиная с любой точки прямоугольника, будет сходиться к решению системы, которое обязательно будет единственным.

Упражнение 73. Докажите предыдущее утверждение.

З а м е ч а н и е. Можно доказать, что решение у подобной системы будет существовать и без выполнения указанного неравенства, но вот метод итераций в этом случае применить не удастся.

Применяя метод итераций, решите следующую задачу.

Упражнение 74. На карту Москвы положили сверху такую же карту, но впятеро меньшего масштаба. Докажите, что можно обе карты проткнуть иглой так, чтобы отверстие изображало на обоих картах одну и ту же точку.

Задачи и упражнения к § 3.7

Английский математик и логик де Морган писал, что после того как Валлис продемонстрировал применение метода Ньютона к уравнению $x^3 - 2x - 5 = 0$, оно стало служить примером каждому изобретателю нового метода численного решения уравнений.

1. Найдите три знака после запятой у корня этого уравнения методом вилки.

Другим знаменитым уравнением, вероятно, первым кубическим уравнением, численно решенным в Европе, является уже упоминавшееся в этой книге уравнение Фибоначчи $x^3 + 2x^2 + 10x = 20$.

2. Найдите решение Фибоначчи $x = 1^\circ 26' 7'' 42'''$ методом Горнера. Естественно, рекомендуется использовать калькулятор, причем для таких задач достаточно простейшего.

3. Найдите девять знаков после запятой у корня уравнений Валлиса и Фибоначчи методом Данделена.

4*. (Валлис.) Методом Ньютона докажите, что корень уравнения

$$x^3 + a(b + a)x - b^3 - 2a^3 = 0$$

при достаточно малом b равен

$$x = a - \frac{b}{4} + \frac{b^2}{64a} + \frac{131b^3}{572a^2} + \dots$$

5*. Если $0,1 \leq N \leq 10$, то

$$|\sqrt{N} - (1 + 4N)/(4 + N)| < 1/12.$$

6*. Докажите, что $\sqrt{N}$ можно вычислить с помощью итераций без деления, если число $M = 1/(2N)$ вычислить заранее. А именно, можно использовать итерации

$$x_{n+1} = x_n \left(\frac{3}{2} - M \cdot x_n^2 \right).$$

Скорость сходимости итераций Ньютона хорошо демонстрирует следующая задача.

7. Если $x_1 = 1$, $x_{n+1} = x_n/2 + 1/x_n$, то

$$0 < x_{10} - \sqrt{2} < 10^{-370}.$$

А следующая задача показывает, как важно выбирать хорошее начальное приближение.

8. Если $x_0 = 10,9$, $x_{n+1} = x_n/2 + 1/x_n$, то $0 < x_{36} - \sqrt{2} < 10^{-9}$.

9. Проверьте, что, применяя метод Ньютона к уравнению $x^2 = x + 1$, можно вычислять десятичные знаки золотого сечения быстрее, чем с помощью цепных дробей.

10*. Проверьте, что применяя метод Ньютона к уравнению $x^2 = x + 1$, начиная с $x_0 = p_0/q_0$, $p_0 = 2$, $q_0 = 1$, получаем итерационную последовательность

$$x_{n+1} = \frac{p_{n+1}}{q_{n+1}} = \frac{x_n^2 + 1}{2x_n - 1} = \frac{p_n^2 + q_n^2}{2p_nq_n - q_n^2},$$

$$p_{n+1} = p_n^2 + q_n^2, \quad q_{n+1} = 2p_nq_n - q_n^2.$$

Докажите по индукции, что

$$p_n = F_{2^n+1}, \quad q_n = F_{2^n}, \quad p_n^2 - p_nq_n - q_n^2 = 1.$$

Покажите, что сложность одновременного вычисления F_{2^n} и F_{2^n+1} не превосходит Cn .

Интересно, что попутно получилась бесконечная последовательность целых решений уравнения $x^2 - xy - y^2 = 1$. Подобные уравнения решаются сведением к так называемому уравнению Пелля.

11.** Пусть α — корень уравнения с целыми коэффициентами

$$a_n x^n + \dots + a_0 = 0$$

(такие числа называются *алгебраическими числами*). Число r назовем ε -приближением к α , если $|r - \alpha| < \varepsilon$. Докажите, что методом Ньютона можно вычислить рациональное ε -приближение к α со сложностью $C \log_2 \log_2 1/\varepsilon$. Под сложностью понимается число арифметических операций, необходимое для его вычисления.

12. Решите методом итераций уравнение $\cos x = x$ с точностью до 5 знаков после запятой.

13. Решите уравнения: (i) $2(2x^2 - 1)^2 - 1 = x$; (ii) $(x^2 - 2)^2 - 2 = x$; (iii) $(x^2 - 1)^2 - 1 = x$.

14. Решите при любом n уравнение $f_n(x) = x$, где (i) $f(x) = x^2 - 2$; (ii) $f(x) = x^2 - 1$; (iii) $f(x) = 2x^2 - 1$.

15. Решите системы

$$1) \begin{cases} \cos x_1 = x_2; \\ \cos x_2 = x_3; \\ \cos x_3 = x_1, \end{cases} \quad 2) \begin{cases} y = x^2 - 2; \\ x = y^2 - 2, \end{cases} \quad 3) \begin{cases} y = 2x^2 - 1; \\ z = 2y^2 - 1; \\ x = 2z^2 - 1, \end{cases} \quad 4) \begin{cases} y = x^2 - 1; \\ z = y^2 - 1; \\ x = z^2 - 1. \end{cases}$$

§ 3.8. Разложение на множители

Начнем с определения.

Определение 82. Многочлен $f(x) \in K[x]$ называется *неприводимым над кольцом K* , если его степень ненулевая и его нельзя представить в виде произведения многочленов над кольцом K степеней, меньших n .

Теорема 83. Пусть F — поле, тогда разложение на неприводимые множители в $F[x]$ всегда существует и однозначно с точностью до перестановок сомножителей и умножения их на константы.

Доказательство. Существование разложения легко доказывается по индукции подобно доказательству существования в теореме 2. $\square$

Для доказательства единственности потребуется

Лемма 20. Если многочлен $p(x)$ неприводим над полем F и делит произведение многочленов $f(x), g(x) \in F[x]$, то $p(x)$ делит либо многочлен $f(x)$, либо многочлен $g(x)$.

Доказательство. Пусть многочлен p не делит g , значит, $(p, g) = 1$, поэтому для некоторых многочленов u, v согласно теореме о линейном представлении НОД справедливо равенство $up + vg = 1$, но тогда многочлен $f = fup + vfg$ делится на многочлен p . $\square$

Из этой леммы индукцией по n легко выводится

Следствие из леммы 20. Если многочлен $p(x)$ неприводим и делит произведение

$$q_1(x)q_2(x) \dots q_n(x),$$

то он делит хотя бы один из сомножителей $q_i(x)$.

Доказательство единственности в теореме 83 проводится индукцией по минимальной длине разложения. База индукции очевидна. Выполним шаг индукции.

Пусть многочлены, разлагающиеся в произведение не более чем n неприводимых многочленов, имеют однозначное разложение, а многочлен $p(x)$ имеет два разложения

$$p(x) = p_1(x)p_2(x) \dots p_{n+1}(x) = q_1(x)q_2(x) \dots q_m(x).$$

Применяя следствие из леммы к многочленам $q_1(x)q_2(x) \dots q_n(x)$ и $p_1(x)$, получаем, что для некоторого i многочлен $p_1(x)$ делит $q_i(x)$, а так как они неприводимы, то $p_1(x) = cq_i(x)$, где c — константа из поля коэффициентов. Тогда, сокращая на $p_1(x)$, получаем два разных разложения одного многочлена, причем первое из них имеет длину n . Полученное противоречие завершает выполнение шага индукции. $\square$

В следующей теореме понадобится

Лемма 21 (Гаусс). НОД коэффициентов произведения $\bar{P}_1(x)$, $\bar{P}_2(x)$ равен единице, если НОД коэффициентов сомножителей равен единице.

Доказательство. Доказательство проведем методом от противного. Пусть

$$\bar{P}_1(x) \cdot \bar{P}_2(x) = a_0 + a_1x + \dots + a_nx^n,$$

$$\bar{P}_1(x) = c_0 + c_1x + \dots + c_mx^m, \quad \bar{P}_2(x) = b_0 + b_1x + \dots + b_kx^k$$

и пусть простое число p делит коэффициенты произведения $\bar{P}_1(x) \cdot \bar{P}_2(x)$. Допустим, что c_t — первый из тех коэффициентов, что не делятся на p . Аналогично выберем b_s для $\bar{P}_2(x)$. Тогда

$$a_{s+t} \equiv b_0c_{s+t} + b_1c_{s+t-1} + \dots + b_{s+t}c_0 \equiv_s c_t \pmod{p},$$

и поэтому p делит b_sc_t , значит, p делит либо b_s , либо c_t — противоречие.

Теорема 84 (Гаусс). У произвольного многочлена $p(x)$ с целыми коэффициентами имеется разложение на множители с рациональными коэффициентами тогда и только тогда, когда $p(x)$ разлагается на множители с целыми коэффициентами.

Доказательство. Из разложимости в $\mathbb{Z}[x]$ вытекает разложимость в $\mathbb{Q}[x]$, так как кольцо $\mathbb{Z}$ содержится в поле $\mathbb{Q}$.

Докажем теорему в обратную сторону. Очевидно, достаточно рассмотреть случай, когда многочлен $P(x)$ есть произведение двух сомножителей (общий случай проверяется по индукции). Пусть $P(x) = P_1(x) \cdot P_2(x)$ — разложение в $\mathbb{Q}[x]$. Представим многочлены в виде

$$P_1(x) = \frac{a_1}{b_1} \hat{P}_1(x), \quad P_2(x) = \frac{a_2}{b_2} \hat{P}_2(x),$$

где $\hat{P}_1(x), \hat{P}_2(x) \in \mathbb{Z}[x]$ и НОД коэффициентов у каждого из многочленов $\hat{P}_1(x), \hat{P}_2(x)$ равен 1. Тогда

$$P(x) = \frac{a_1 a_2}{b_1 b_2} \hat{P}_1(x) \hat{P}_2(x),$$

где $\frac{a_1 a_2}{b_1 b_2} \in \mathbb{Z}$, потому что коэффициенты многочлена $P(x)$ целые, а НОД коэффициентов многочленов $\hat{P}_1(x), \hat{P}_2(x)$ равен 1 согласно предыдущей лемме. $\square$

Следствие из теоремы 84. *Многочлен с целыми коэффициентами неприводим в кольце $\mathbb{Z}[x]$ тогда и только тогда, когда он неприводим в кольце $\mathbb{Q}[x]$. Разложение на неприводимые множители в кольце $\mathbb{Z}[x]$ однозначно с точностью до перестановки множителей и их умножения на константы.*

Для быстрого тестирования неприводимости в некоторых случаях полезны следующие *достаточные признаки неприводимости*.

Теорема 85 (редуктивный признак неприводимости). *Многочлен*

$$f(x) = a_n + a_1 x + \dots + a_n x^n \in \mathbb{Z}[x]$$

неприводим, если $\bar{a}_n$ не кратно p и многочлен

$$\bar{f}(x) = \bar{a}_0 + \bar{a}_1 x + \dots + \bar{a}_n x^n,$$

где $\bar{a}_i = a_i \bmod p$, неприводим над полем $\mathbb{Z}_p$.

Доказательство. Пусть $f(x) = g(x) \cdot h(x)$ — разложение на множители в кольце $\mathbb{Z}[x]$. Тогда $\bar{f}(x) = \bar{g}(x) \cdot \bar{h}(x)$ — разложение в кольце $\mathbb{Z}_p$. $\square$

Теорема 86 (признак Эйзенштейна*). *Пусть многочлен*

$$f(x) = a_0 + a_1 x + \dots + a_n x^n \in \mathbb{Z}[x]$$

* Ф. Эйзенштейн (Ferdinand Gotthold Max Eisenstein, 1823–1852) — выдающийся немецкий математик.

таков, что a_n не кратно простому числу p , и p делит остальные коэффициенты $a_0, a_1, \dots, a_{n-1}$, но p^2 не делит a_0 . Тогда $f(x)$ неприводим.

Доказательство. Пусть

$$f(x) = g(x) \cdot h(x), \quad g(x) = b_0 + b_1x + \dots + b_kx^k, \\ h(x) = c_0 + c_1x + \dots + c_mx^m,$$

значит, p не делит $b_kc_m = a_n$, а $b_0c_0 = a_0$ делится на p , но не делится на p^2 , поэтому одно из них не делится на p , например b_0 , а тогда c_0 делится на p .

Заметим, что p делит c_1 . В самом деле, p делит $a_1 = b_0c_1 + c_0b_1$, следовательно, $p \mid b_0c_1$, а значит, согласно лемме 1 § 1.2 $p \mid c_1$. Аналогично p делит $a_2 = b_0c_2 + b_1c_1 + b_2c_0$, следовательно, $p \mid c_2$ и т. д. и, наконец, $p \mid a_m = b_0c_m + b_1c_{m-1} + \dots + b_mc_0$, следовательно, $p \mid c_m$, что невозможно, так как тогда p делит $b_kc_m = a_n$. $\square$

Упражнение 75. 1. Многочлены $x^m - p$, где p — простое, и $x^m - p_1 \dots p_k$, где p_i — различные простые, неприводимы согласно критерию Эйзенштейна (и, следовательно, число $\sqrt[m]{p}$ иррационально).

2. Многочлен деления круга

$$f_p(x) = x^{p-1} + x^{p-2} + \dots + x + 1 = 0$$

неприводим. Действительно, $f_p(x) = \frac{x^p - 1}{x - 1}$ неприводим тогда и только тогда, когда $f_p(x + 1)$ неприводим. Но

$$f_p(x + 1) = \frac{(x + 1)^p - 1}{x + 1 - 1} = x^{p-1} + C_p^{p-1}x^{p-2} + \dots + C_p^2x + C_p^1,$$

все его коэффициенты C_p^k , $k \geq 1$, кратны p , а свободный член $C_p^1 = p$ не кратен p^2 , значит, согласно критерию Эйзенштейна, многочлен $f_p(x + 1)$ неприводим.

Указанные признаки неприводимости хотя и просты, но не всегда применимы. Опишем алгоритм, называемый *алгоритмом Кронекера*, который позволяет для любого многочлена над полем рациональных чисел не только выяснить, является ли он неприводимым, но и указать разложение его на множители, если он приводим. Однако, как будет видно, этот алгоритм приводит к очень громоздким вычислениям, хотя в отдельных случаях его можно применять с успехом.

Если дан многочлен $f(x) \in \mathbb{Z}[x]$, $\deg f = n$, то тестирование его неприводимости и разложение на множители сводятся к поиску делителя $g(x)$

заданной степени k . В случае $k = 1$ этот алгоритм уже был изложен в задаче 11 из § 3.2. Можно считать, что $k \leq n/2$, так как в случае $k > n/2$ вместо g можно искать $h = f/g$, $\deg h = n - k < n/2$.

Пусть такой делитель существует. Согласно теореме 84 можно полагать, что $f, g, h = f/g \in \mathbb{Z}[x]$. Возьмем произвольный набор различных целых чисел $\{a_0, \dots, a_k\}$ и вычислим $f(a_i) \in \mathbb{Z}$, $i = 0, \dots, k$. Тогда

$$g(a_i), h(a_i) \in \mathbb{Z}, \quad f(a_i) = g(a_i)h(a_i), \quad i = 0, \dots, k,$$

поэтому $g(a_i) \mid f(a_i)$, $i = 0, \dots, k$. Для каждого числа $f(a_i)$, $i = 0, \dots, k$ составим список D_i всех его *целых* делителей.

Для каждого i выберем $d_i \in D_i$ и, решив задачу интерполяции, найдем многочлен $g_j \in \mathbb{Q}[x]$. Если $g_j \in \mathbb{Z}[x]$, то проверяем, делится ли $f(x)$ на $g_j(x)$. Если нет, то выбираем другой набор значений

$$(d_0, d_1, \dots, d_k) \in D_0 \times \dots \times D_k,$$

и для него повторяем ту же процедуру, пока не найдем делитель. В случае неудачи можно сделать вывод об отсутствии делителя степени k и перейти к поиску делителя степени $k + 1$ и т.д. Если делитель не будет найден, значит, многочлен неприводим.

Очевидно, что перебор вариантов

$$(d_0, d_1, \dots, d_k) \in D_0 \times \dots \times D_k$$

можно ограничить только наборами с НОД, равным единице, причем d_0 можно выбирать только положительным.

Чтобы уменьшить этот перебор, можно выбирать множество $\{a_0, \dots, a_k\}$ так, чтобы числа $f(a_i) \in \mathbb{Z}$, $i = 0, \dots, k$, имели бы по возможности меньшее число различных делителей, например, были бы простыми числами или еще лучше плюс-минус единицами. С целью упрощения дальнейшей интерполяции удобно выбирать числа $\{a_0, \dots, a_k\}$ по возможности малыми, в лучшем случае брать $\{a_0, \dots, a_k\} = \{0, \pm 1, \pm 2, \dots\}$. Можно пользоваться интерполяционными формулами как Ньютона, так и Лагранжа.

Упражнение 76. Разложите на множители многочлен

$$2x^5 + 8x^4 - 7x^3 - 35x^2 + 12x - 1.$$

У к а з а н и е. Находим, что $f(0) = -1$, $f(2) = 19$, $f(-3) = -1$. Тогда

$$d_0 = 1; \quad d_1 = \pm 1, \pm 19; \quad d_2 = \pm 1.$$

Ищем $g(x)$ в виде $c_0 + c_1x + c_2x(x-2)$. Тогда

$$c_0 = 1, \quad 1 + 2c_1 = d_1, \quad 1 - 3c_1 + 15c_2 = d_2 = \pm 1,$$

откуда $d_2 = 1$, $c_1 = 5c_2$, $d_1 = -19$, $c_1 = -10$, $c_2 = -2$ (случай $d_1 = 1$ дает $c_1 = 0 = c_2$), значит, $g(x) = 1 - 10x - 2x(x - 2) = -2x^2 - 6x + 1$ — единственное нетривиальное решение. Выполняя деление, находим, что

$$2x^5 + 8x^4 - 7x^3 - 35x^2 + 12x - 1 = (2x^2 + 6x - 1)(x^3 + x^2 - 6x + 1).$$

Сравнительно недавно был найден* достаточно быстрый алгоритм разложения на множители над кольцом целых чисел, сложность которого ограничивается многочленом от суммарного количества цифр его коэффициентов, но он слишком сложен для понимания, чтобы излагать его здесь.

Более простые для понимания и более быстрые алгоритмы разложения (или, как еще говорят, *факторизации*) еще в 60-е годы XX в. были найдены** для многочленов над конечными полями. Эти алгоритмы имеют важные приложения, в частности в теории кодирования.

Задачи и упражнения к § 3.8

1. Докажите с помощью критерия Эйзенштейна неприводимость над полем рациональных чисел многочленов

- а) $x^4 - 8x^3 + 12x^2 - 6x + 2$; в) $x^4 - x^3 + 2x + 1$;
 б) $x^5 - 12x^3 + 36x - 12$; г) $x^5 - 3x^4 + 6x^3 - 3x^2 + 9x - 6$.

2. Составьте таблицу неприводимых многочленов над полем $\mathbb{Z}_2$ до десятой степени включительно.

3. Составьте таблицу неприводимых многочленов над полем $\mathbb{Z}_3$ до пятой степени включительно.

4. Докажите с помощью редукции по модулю 2 неприводимость над $\mathbb{Q}$ многочлена $x^5 + 2x^3 + 3x^2 - 6x - 5$.

5. Докажите с помощью редукции по модулям 2 и 3 неприводимость над $\mathbb{Q}$ многочлена $x^5 - 6x^3 + 2x^2 - 4x + 5$.

6. Многочлен $x^4 + ax^3 + bx^2 + cx + d$ с целыми коэффициентами неприводим над $\mathbb{Q}$, если он не имеет целых корней и не делится ни на один из многочленов вида $x^2 + x(ct - am^2)/(d - m^2) + m$, где $m \mid d$ (многочлены с дробными коэффициентами можно не принимать во внимание). Исключение могут составлять многочлены, у которых $d = k^2$, $c = ak$.

* Л.Ловасом и Х.Ленстрой.

** Э. Берлекэмпом.

7. Многочлен $x^5 + ax^4 + bx^2 + cx + dx + e$ с целыми коэффициентами неприводим над $\mathbb{Q}$, если он не имеет целых корней и не делится ни на один из многочленов с целыми коэффициентами вида

$$x^2 + x \frac{am^3 - cm^2 - dn + be}{m^3 - n^2 + ae - dm} + m,$$

где $m \mid e$, $n = e/m$.

8. Применяя предыдущие задачи, разложите на множители над $\mathbb{Q}$ или докажите неприводимость многочленов

- а) $x^4 - 3x^3 + 2x^2 + 2x - 6$; в) $x^5 + x^4 - 4x^3 + 9x^2 - 6x + 6$.
 б) $x^4 - 3x^3 + 2x^2 + 2x - 6$;

9. При каком значении a многочлен $x^{13} + x + 90$ делится на $x^2 - x + a$?

У к а з а н и е. Применить теорему Гаусса и алгоритм Кронекера.

10*. Докажите неприводимость над $\mathbb{Q}$ многочленов при различных $a_i \in \mathbb{Z}$:

- а) $(x - a_1) \dots (x - a_n) - 1$;
 б) $(x - a_1)^2 \dots (x - a_n)^2 + 1$;
 в) $(x - a_1) \dots (x - a_n) + 1$, за исключением случаев $n = 4$, $a_2 = a_1 + 1$, $a_3 = a_2 + 1$, $a_4 = a_3 + 1$ и $n = 2$, $a_2 = a_1 + 2$.

У к а з а н и е. Применить алгоритм Кронекера.

11. Если $f(x) \in \mathbb{Z}[x]$ и уравнение $f(x) = 1$ имеет не менее четырех целых корней, то уравнение $f(x) = -1$ не имеет целых корней.

У к а з а н и е. Применить алгоритм Кронекера.

12*. Если $f(x) \in \mathbb{Z}[x]$ и уравнение $f^2(x) = 1$ имеет более чем $n/2$ целых корней, то при $n \geq 12$ многочлен $f(x)$ неприводим над $\mathbb{Q}$.

У к а з а н и е. Применить алгоритм Кронекера.

13*. Если $f(x) \in \mathbb{Z}[x]$, то найдется такой многочлен $g(x) \in \mathbb{Z}[x]$, что многочлен $f(g(x))$ приводим над кольцом $\mathbb{Z}$.

14*. Найдите все n , при которых многочлен $x^n + 4$ разлагается на множители с целыми коэффициентами.

15*. Докажите, что в кольце $\mathbb{Z}[x]$ многочлен $\frac{x^{mn} - 1}{x^m - 1}$ делится на многочлен $\frac{x^n - 1}{x - 1}$, если m и n взаимно просты.

16*. Докажите, что число $\frac{a^{mn} - b^{mn}}{a^m - b^m}$ делится на число $\frac{a^n - b^n}{a - b}$, если m и n взаимно просты.

§ 3.9. Взаимные многочлены

Далее рассматриваем многочлены над произвольным полем.

Определение 83. Два многочлена $f(x)$, $g(x)$ равной степени n назовем *взаимными*, если их коэффициенты связаны равенствами $a_k = b_{n-k}$, $k = 0, \dots, n$. В этом случае будем писать $f = g^*$ или $g = f^*$.

Примеры. 1. Многочлены $1 + x + 2x^2$, $2 + x + x^2$ взаимные.
2. Многочлены $1 + x + 2x^2 + 3x^3$, $3 + 2x + x^2 + x^3$ тоже взаимны друг другу.

3. Очевидно, $f^{**} = f$.

Упражнение 77. 1. Проверьте, что $f = g^* \iff f(x) = g(1/x)x^{\deg g}$.

2. Если $\deg f = \deg g$, то $(f \pm g)^* = f^* \pm g^*$.

3. Если $\deg f \neq \deg g$, то предыдущее утверждение неверно.

Определение 84. Многочлен f называется *возвратным*, если $f = f^*$.

Примеры. 1. Многочлен $1 + x + x^2 + \dots + x^n$ возвратный.

2. Многочлен $1 + x + 2x^2 + x^3 + x^4$ тоже.

3. Константа — возвратный многочлен.

Справедлива следующая очевидная

Теорема 87.

(i) *Справедливо тождество $(fg)^* = f^*g^*$.*

(ii) *Произведение возвратных многочленов — возвратный многочлен.*

(iii) *Взаимные многочлены одновременно либо неприводимы, либо приводимы.*

Доказательство. Утверждение (i) следует из тождества

$$x^{\deg f} f(1/x) x^{\deg g} g(1/x) = x^{\deg f + \deg g} f(1/x) g(1/x) = x^{\deg fg} fg(1/x).$$

Утверждение (ii) следует из (i). Утверждение (iii) тоже следует из (i). $\square$

Лемма 22. *Существует единственный многочлен $P_n(x)$ такой, что $P_n(x + 1/x) = x^n + x^{-n}$.*

Доказательство. База индукции ($n = 1, 2$) очевидна, так как $P_2(x) = x^2 - 2$. Шаг индукции обосновывается тождеством

$$x^{n+1} + x^{-n-1} = (x^n + x^{-n})(x + x^{-1}) - x^{n-1} + x^{-n+1},$$

если определить последовательность $P_n(x)$ рекуррентным соотношением

$$P_{n+1} = xP_n(x) - P_{n-1}(x).$$

$\square$

Теорема 88 (Муавр). (i) Если f — возвратный многочлен степени $2n$, то

$$x^{-n}f(x) = F_n(x + \frac{1}{x}),$$

где F_n — многочлен степени n .

(ii) Если f — возвратный многочлен степени $2n + 1$, то $\frac{f(x)}{(x+1)}$ — возвратный многочлен степени $2n$.

Доказательство. Доказательство (i) основано на тождестве

$$x^{-n}f(x) = \sum_{k=0}^n a_k(x^k + x^{-k}) = \sum_{k=0}^n a_k P_k(x + \frac{1}{x}),$$

и в качестве F_n берем

$$\sum_{k=0}^n a_k P_k(x).$$

Доказательство (ii) основано на тождестве

$$\frac{f(x)}{x+1} = g(x) = \sum_{k=0}^n a_k \frac{x^k + x^{2n+1-k}}{1+x} = \sum_{k=0}^n a_k q_k$$

и замечания, что, хотя многочлены q_k и не возвратные, но

$$q_k = \frac{x^k + x^{2n+1-k}}{1+x} = x^k - x^{k+1} + \dots - x^{2n-k-1} + x^{2n-k}$$

и их коэффициенты удовлетворяют равенствам $a_k = a_{2n-k}$, значит, и многочлен $g(x)$ тоже удовлетворяет этим равенствам и является возвратным, так как его степень равна $2n$. $\square$

Следствие из теоремы 88. Возвратное уравнение n -й степени сводится к уравнению степени $\lfloor n/2 \rfloor$.

Определение 85. Многочлен $p(x)$ называется *четным*, если он удовлетворяет тождеству $p(x) = p(-x)$, и *нечетным*, если он удовлетворяет тождеству $p(x) = -p(-x)$.

Упражнение 78. 1. Любой многочлен однозначно представим в виде суммы четного и нечетного многочленов.

2. Четный многочлен степени n представим в виде $f(x^2)$, где f — многочлен степени $n/2$ и содержит только четные степени, а нечетный — в виде $xf(x^2)$, где f — многочлен степени $(n-1)/2$ и содержит только нечетные степени.

3. Четное или нечетное уравнение n -й степени сводится к уравнению степени $\lfloor n/2 \rfloor$.

Задачи и упражнения к § 3.9

1. Решите уравнения

(i) $x^3 + 3x^2 - 5x + 3x + 1 = 0$;

(ii) $x^4 + 2x^3 - 4x^2 + 2x + 1 = 0$.

2. Многочлены Чебышёва определяются равенством $T_n(\cos x) = \cos nx$. Докажите, что $P_n(x) = 2T_n(x/2)$.

Последовательность $P_i(x)$ можно формально продолжить и для отрицательных индексов, при этом, очевидно $P_{-i}(x) = P_i(x)$.

3. Многочлены P_n с четными номерами сами четные, а многочлены с нечетными номерами — сами нечетные. Поэтому их удобно представлять в виде

$$P_i(x) = \sum_{j=0}^{\lfloor i/2 \rfloor} a_{i,j} (-1)^j x^{i-2j}.$$

4. Для последовательности $P_n(x)$ справедливо тождество

$$P_{nm}(x) = P_n(P_m(x)) = P_m(P_n(x)).$$

У к а з а н и е. Положите $x = z + z^{-1}$, тогда

$$P_n(P_m(z + z^{-1})) = P_n(z^m + z^{-m}) = z^{nm} + z^{-nm} = P_{nm}(z + z^{-1}).$$

5. Для последовательности $P_n(x)$ справедливо тождество

$$P_{n+m}(x) + P_{n-m}(x) = P_n(x)P_m(x).$$

У к а з а н и е. Действительно,

$$z^{n+m} + z^{-n-m} + z^{n-m} + z^{-n+m} = (z^n + z^{-n})(z^m + z^{-m}).$$

6*. Для последовательности $P_n(x)$ справедливы следующие равенства

(i) $P_i(x) = \sum_{j=0}^{\lfloor i/2 \rfloor} a_{i,j} (-1)^j x^{i-2j}, \quad a_{i,j} = C_{i-j}^j + C_{i-j-1}^{j-1},$

(ii) $x^i = \sum_{j=0}^{\lfloor i/2 \rfloor} C_i^j P_{i-2j}$, где для удобства положим $P_0 = 1$.

У к а з а н и е. База индукции проверяется непосредственно. Для обоснования шага индукции ввиду тождества

$$P_{i+1}(x) = xP_i(x) - P_{i-1}(x)$$

достаточно проверить, что всегда $a_{i+1,j} = a_{i,j} + a_{i-1,j-1}$, а это вытекает из тождества Паскаля:

$$a_{i,j} + a_{i-1,j-1} = C_{i-j}^j + C_{i-j-1}^{j-1} + C_{i-j}^{j-1} + C_{i-j-1}^{j-2} = C_{i+1-j}^j + C_{i-j}^{j-1} = a_{i+1,j}.$$

$$\begin{aligned} x^{i+1} &= x x^i = \sum_{j=0}^{\lfloor i/2 \rfloor} C_i^j x P_{i-2j} = \sum_{j=0}^{\lfloor i/2 \rfloor} C_i^j (P_{i-2j+1} + P_{i-2j-1}) = \\ &= P_{i+1} + \sum_{j=1}^{\lfloor i/2 \rfloor} (C_i^j + C_i^{j-1}) P_{i-2j-1} = \sum_{j=0}^{\lfloor i/2 \rfloor} C_{i+1}^j P_{i-2j+1}. \end{aligned}$$

Пусть K — кольцо. Напомним, что через $K[x_1, \dots, x_n]$ обозначается кольцо многочленов от переменных $x_1, \dots, x_n$ с коэффициентами из кольца K .

$$f(x_1, \dots, x_n) = \sum_{i_1 \dots i_n} a_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n} \in K[x_1, \dots, x_n]$$

Определение 86. Определим действие перестановки α на многочлен f равенством

$$f_{\alpha}(x_1, \dots, x_n) = \sum_{i_1 \dots i_n} a_{i_1 \dots i_n} x_{\alpha^{-1}(1)}^{i_1} \dots x_{\alpha^{-1}(n)}^{i_n}.$$

Определение 87. Многочлен $f(x_1, \dots, x_n) \in K[x_1, \dots, x_n]$ называется *симметрическим*, если для любой перестановки $\alpha \in S_n$ справедливо равенство

$$f_\alpha(x_1, \dots, x_n) = f(x_1, \dots, x_n).$$

Определение 88. *Элементарные симметрические многочлены* — это многочлены

$$\begin{aligned} \sigma_1(x_1, \dots, x_n) &= x_1 + \dots + x_n, \\ \sigma_2(x_1, \dots, x_n) &= x_1x_2 + x_1x_3 + \dots + x_1x_n + x_2x_3 + \dots + x_{n-1}x_n, \\ &\dots\dots\dots \\ \sigma_k(x_1, \dots, x_n) &= x_1x_2 \dots x_k + \dots + x_{n-k+1} \dots x_n, \\ &\dots\dots\dots \\ \sigma_n(x_1, \dots, x_n) &= x_1 \dots x_n. \end{aligned}$$

Упражнение 79. Симметрический многочлен можно записывать в виде

$$f(x_1, \dots, x_n) = \sum_{i_1 \leq i_2 \leq \dots \leq i_n} a_{i_1 \dots i_n} (x_1^{i_1} \dots x_n^{i_n} + \dots),$$

Теорема 89 (Виет*). Многочлен

имеет n (не обязательно различных) корней $x_1, \dots, x_n$ тогда и только тогда, когда выполняется система равенств

Доказательство заключается в раскрытии скобок в произведении $f(z) = (z - x_1)(z - x_2) \dots (z - x_n)$. Получаем равенство

Если два многочлена равны, то равны их коэффициенты. Поэтому

Теорема 90 (о симметрических многочленах). *Предположим, что $f(x_1, \dots, x_n)$ — симметрический многочлен. Тогда существует и притом только один многочлен $\varphi(y_1, \dots, y_n)$ такой, что*

Доказательство. Докажем существование такого многочлена. Достаточно сделать это для симметрических многочленов вида $x_1^{i_1} \dots x_n^{i_n} + \dots$. Всяду в дальнейшем будем выписывать только одно слагаемое, предполагая, что в сумму включены и все другие слагаемые, получающиеся из него перестановками переменных.

Можно считать, что $i_1 \geq i_2 \geq \dots \geq i_n$. Будем говорить, что одночлен $x_1^{i_1} \dots x_n^{i_n}$ старше одночлена $x_1^{j_1} \dots x_n^{j_n}$ (имеет больший вес), если выполняется неравенство

* Ф. Виет (François Viète, 1540–1603) — выдающийся французский математик, придворный криптоаналитик Генриха IV, по основной профессии — юрист.

или выполняется равенство

$$i_1 + \dots + i_n = j_1 + \dots + j_n$$

и одно из следующих условий:

$$\begin{aligned} i_1 &> j_1; \\ i_1 &= j_1, \quad i_2 > j_2; \end{aligned}$$

и т. д. Записываем отношение старшинства в виде

$$x_1^{i_1} \dots x_n^{i_n} \gg x_1^{j_1} \dots x_n^{j_n}.$$

Будем выражать симметрические многочлены $x_1^{i_1} \dots x_n^{i_n} + \dots$ через элементарные симметрические многочлены и симметрические многочлены вида $x_1^{j_1} \dots x_n^{j_n} + \dots$, где $x_1^{i_1} \dots x_n^{i_n} \gg x_1^{j_1} \dots x_n^{j_n}$. Заметим, что при раскрытии скобок в произведении

$$\sigma_1^{i_1-i_2} \sigma_2^{i_2-i_3} \dots \sigma_{n-1}^{i_{n-1}-i_n} \sigma_n^{i_n}$$

в сумме будет присутствовать одночлен вида $x_1^{i_1} \dots x_n^{i_n}$ (и все одночлены, получающиеся из него перестановками переменных). При этом среди одночленов в этой сумме он будет старшим. Тогда у симметрического многочлена

$$x_1^{i_1} \dots x_n^{i_n} + \dots - \sigma_1^{i_1-i_2} \sigma_2^{i_2-i_3} \dots \sigma_{n-1}^{i_{n-1}-i_n} \sigma_n^{i_n}$$

все одночлены имеют меньший вес. Для каждого из них применим ту же процедуру. Продолжая этот процесс, мы выразим наш многочлен через элементарные симметрические многочлены за конечное число шагов.

Доказательство единственности этого выражения проведем от противного. Пусть

$$\varphi_1(\sigma_1(x_1, \dots, x_n), \dots, \sigma_n(x_1, \dots, x_n)) \quad \text{и} \quad \varphi_2(\sigma_1(x_1, \dots, x_n), \dots, \sigma_n(x_1, \dots, x_n))$$

— два различных выражения для $f(x_1, \dots, x_n)$. Тогда ненулевой многочлен

$$\varphi(y_1, \dots, y_n) = \varphi_1(y_1, \dots, y_n) - \varphi_2(y_1, \dots, y_n)$$

при подстановке $y_i = \sigma_i(x_1 \dots x_n)$ обращается в нуль. При этой подстановке одночлен $ay_1^{j_1} y_2^{j_2} \dots y_n^{j_n}$ в многочлене $\varphi(y_1 \dots y_n)$ с ненулевым коэффициентом a перейдет в сумму одночленов, в которой старшим будет одночлен

$$ax_1^{j_1+\dots+j_n} \dots x_{n-1}^{j_{n-1}+j_n} x_n^{j_n}.$$

Упражнение. Докажите это.

Из всех одночленов $ay_1^{j_1} \dots y_n^{j_n}$ многочлена $\varphi(y_1 \dots y_n)$ выберем такой, что одночлен

$$ax_1^{j_1+\dots+j_n} \dots x_{n-1}^{j_{n-1}+j_n} x_n^{j_n}$$

будет самым старшим из всех возможных.

Упражнение. Докажите, что такой выбор возможен.

Тогда при подстановке элементарных симметрических многочленов в многочлен $\varphi(y_1, \dots, y_n)$ этот многочлен будет старшим в полученном многочлене. Поэтому ему не с чем будет сократиться и $\varphi(\sigma_1, \dots, \sigma_n) \neq 0$. Противоречие. $\square$

Симметрические многочлены и доказанная теорема имеют много приложений. Например, ее использование облегчает решение симметрических систем уравнений.

Определение 89. Система называется *симметрической*, если ее легко преобразовать к виду, состоящему из симметрических многочленов.

С помощью упоминавшейся теоремы симметрическую систему можно свести путем замены переменных к несимметрической, но, как правило, более простой системе, а для нахождения исходных переменных решить систему Виета, которая в случае двух переменных выглядит так:

$$\begin{cases} x + y = u; \\ xy = v, \end{cases}$$

а в случае, например, трех переменных выглядит так:

$$\begin{cases} x + y + z = u; \\ xy + xz + yz = v; \\ xyz = w. \end{cases}$$

Ее решение с помощью теоремы Виета сводится к решению соответствующего алгебраического уравнения.

В качестве еще одного приложения симметрических многочленов рассмотрим метод приближенного нахождения корней уравнений, известный иногда под не вполне вразумительным, но коротким названием метода квадратного корня. Этот метод независимо был открыт Данделеном, Лобачевским*, Греффе и Энке. Он приложим только к алгебраическим уравнениям и требует большего объема вычислений, чем метод Ньютона, но зато вычисляет сразу все корни уравнения, в том числе и комплексные, и даже может определить их кратность, причем не требует предварительного деления корней и нахождения их приближений с невысокой точностью, как метод Ньютона.

Основная идея заключается в том, что мы можем, используя теорему Виета и теорему о симметрических многочленах, построить для любого

* Лобачевский изложил его в своем учебнике «Алгебра, или вычисление конечных», изданном в Казани в 1834 г.

уравнения

$$x^n + a_1 x^{n-1} + \dots + a_n = 0$$

новое уравнение

$$x^n + b_1 x^{n-1} + \dots + b_n = 0,$$

у которого все корни являются заданной m -й степенью корней исходного уравнения. Для простоты предположим, что модули всех его корней различны:

$$|x_1| > |x_2| > \dots > |x_n|.$$

Впрочем, если мы предварительно проведем отделение кратных корней, как будет показано в § 3.12, вероятность появления равных модулей будет очень мала.

Если m достаточно велико, то $|x_1^m|$ будет значительно больше $|x_2^m|$, поэтому можно считать, что

$$|b_1| = |\sigma_1(x_1^m, \dots, x_n^m)|$$

приближенно равно $|x_1^m|$, откуда имеем приближенную формулу

$$\ln |x_1| \approx \frac{1}{m} \ln |b_1|.$$

Аналогично находим модули остальных корней, например, для нахождения $|x_2|$ замечаем, что если m достаточно велико, то $|x_1^m x_2^m|$ будет значительно больше всех остальных $|x_i^m x_j^m|$, поэтому можно считать, что

$$|b_2| = |\sigma_2(x_1^m, \dots, x_n^m)|$$

приближенно равно $|x_1^m x_2^m|$, откуда имеем приближенную формулу

$$\ln |x_1 x_2| = \frac{1}{m} \ln |b_2|,$$

а так как $|x_1|$ уже найден, то приближенно

$$\ln |x_2| = \frac{1}{m} (\ln |b_2| - \ln |b_1|)$$

и т. д.

Однако находить указанное уравнение для очень больших m чрезвычайно трудоемко, и кажется, что это обесценивает идею. Но можно делать это только для $m = 2^k$, k раз повторяя процедуру построения уравнения, корни которого равны квадратам корней исходного (применяем бинарный метод!). Еще некоторое упрощение вычислений достигается введением понятия *корней Энке*.

Определение 90. *Корнями Энке* назовем корни уравнения, взятые с обратным знаком.

Очевидно, что квадраты корней Энке совпадают с квадратами обычных корней, а теорема Виета для корней Энке приобретает особенно простой вид, так как в ней можно не следить за знаками коэффициентов.

На каждом шаге итерации будем по исходному уравнению

$$x^n + a_1x^{n-1} + \dots + a_n = 0$$

строить новое уравнение

$$x^n + b_1x^{n-1} + \dots + b_n = 0,$$

у которого корни Энке являются квадратами корней Энке исходного уравнения. Для этого в исходном уравнении перенесем нечетные степени в правую часть, возведем полученное уравнение почленно в квадрат (далее в выкладках для определенности положим, что n — четно)

$$(x^n + a_2x^{n-2} + a_4x^{n-4} + \dots)^2 = (a_1x^{n-1} + a_3x^{n-3} + \dots)^2$$

и введем новую переменную, полагая $y = -x^2$, откуда имеем

$$y^n + (a_1^2 - 2a_2)y^{n-1} + (a_2^2 - 2a_1a_3 + 2a_4)y^{n-2} + \dots = 0.$$

У полученного уравнения корни Энке как раз и равны квадратам корней Энке исходного уравнения.

Упражнение 80. Проверьте, что остальные коэффициенты нового уравнения вычисляются по формулам

$$\begin{aligned} b_3 &= a_3^2 - 2a_2a_4 + 2a_1a_5 - 2a_6, \\ b_4 &= a_4^2 - 2a_3a_5 + 2a_2a_6 - 2a_1a_7 + 2a_8, \\ &\dots\dots\dots, \\ b_n &= a_n^2, \end{aligned}$$

и покажите, что сложность вычисления коэффициентов оценивается как $3n^2/2 + Cn$ операций сложения-вычитания и умножения чисел, где C — некоторая константа.

Правило вычисления коэффициентов может быть выражено словесно следующим образом: i -й коэффициент нового уравнения получается прибавлением к квадрату i -го коэффициента исходного уравнения удвоенного произведения каждой пары коэффициентов, равноотстоящих от него с обеих сторон и взятых с чередующимися знаками.

Если нужно найти корни уравнения, например, с четырьмя знаками после запятой, но допускается, что точность вычисления может быть и меньше, то можно все вычисления делать с четырьмя знаками и для краткости записывать получающиеся очень большие коэффициенты в виде, например, 2002^p вместо $2002 \cdot 10^p$.

Приведем пример * вычисления корней уравнения $f(x) = x^3 + 9x^2 + 23x + 14 = 0$. Для краткости уравнение, полученное из f одним шагом итерации, обозначаем f^2 , следующее уравнение обозначаем f^4 и т. д. Вычисления прекращаем, когда квадраты коэффициентов уравнения f^{2^k} совпадают (при применяемой точности вычислений) с коэффициентами уравнения $f^{2^{k+1}}$.

Расположим сначала коэффициенты уравнения в следующем порядке:

x^3	x^2	x^1	x^0
1	9000^{-3}	2300^{-2}	1400^{-2}

На каждом шаге вычисления возводим в квадрат эти коэффициенты и прибавляем удвоенные произведения согласно приведенному правилу, располагая вычисления в таблицу *.

	1	8100^{-2} -4600	5290^{-1} -2520	1960^{-1}
f^2	1	3500^{-2} 1225^0 -0554	2770^{-1} 7673^1 -1372	1960^{-1} 3842^1
f^4	1	0671^0 4502^2 -1260	6301^1 3970^6 -0052	3842^1 1476^6

f^8	1	3242^2 1051^8 -0078	3918^6 1535^{16}	1476^6 2179^{15}
f^{16}	1	0973^8 9467^{18} -0031	1535^{16} 2356^{35}	2179^{15} 4748^{33}
f^{32}	1	9436^{18}	2356^{35}	4748^{33}
f^{64}	1	8904^{40}	5551^{73}	2254^{70}

На этом шаге вычисление заканчивается. Находим теперь модули корней согласно указанным выше правилам:

$$|x_1| = 4,861, \quad |x_2| = 3,254, \quad |x_3| = 0,8851.$$

Знаки корней можно определить, подставляя оба варианта в уравнение (используя при этом схему Горнера).

Заметим, что в приведенных рассуждениях можно считать корни также и комплексными числами, при этом приближенно вычисляются их модули. Метод квадратного корня можно приспособить и для нахождения аргументов комплексных корней, при этом корни будут найдены полностью.

* Заимствованный из прекрасной книги Э. Уитткера и Г. Робинсона «Математическая обработка результатов наблюдений» (ОНТИ, 1935).

* Раньше для этого использовали таблицы возведения в квадрат и таблицы логарифмов или логарифмические линейки, а сейчас их заменяет калькулятор.

Задачи и упражнения к § 3.10

1. Выразите через элементарные симметрические функции
 - а) $x^3 + y^3 + z^3 - 3xyz$; в) $\sum 1/x_i$ и $\sum 1/x_i^2$;
 - б) $(x-y)^2(x-z)^2(y-z)^2$; г) $\sum x_i^2 x_j^2$.
2. Пусть x_i — корни уравнения $ax^2 + bx + c = 0$. Выразите через a, b, c величины $x_1^3 + x_2^3$ и $x_1^{-3} + x_2^{-3}$.
3. Пусть x_i — корни уравнения $x^4 - 7x^3 + 1 = 0$. Составьте для $i = 1, \dots, 4$ уравнение с корнями (i) x_i^2 , (ii) x_i^4 , (iii) x_i^8 , (iv) x_i^{16} .
4. Решите методом квадратного корня уравнение $x^2 - 3x + 2 = 0$.
- 5*. Решите методом квадратного корня уравнение с кратными корнями $x^3 + 7x^2 + 16x + 12 = 0$.
- 6*. Пусть x_i — корни уравнения золотого сечения $x^2 - x - 1 = 0$. Составьте уравнение с корнями $x_i^{2^n}$, $i = 1, 2$.
- 7*. Пусть x_i — корни уравнения $x^{2005} - 7x^3 + 1 = 0$. Найдите сумму $\sum_{i=1}^{2005} x_i^{2005}$.
8. Решите систему уравнений

$$\begin{cases} x^3y + x^3y^2 + 2x^2y^2 + x^2y^3 + xy^3 = 30; \\ x^2y + xy + x + y + xy^2 = 11. \end{cases}$$

9. Решите систему уравнений

$$\begin{cases} \frac{x+y}{1+xy} = \frac{5}{4}; \\ \frac{x^4+y^4}{1+x^4y^4} = \frac{257}{32}. \end{cases}$$

10*. Обозначим через $s_k = x_1^k + \dots + x_n^k$ степенные суммы и через $\sigma_k = \sum x_1 \dots x_k$ элементарные симметрические многочлены. Докажите формулы Ньютона:

$$\begin{cases} s_k - s_{k-1}\sigma_1 + \dots + (-1)^n s_{k-n}\sigma_n = 0 & \text{при } k > n, \\ s_k - s_{k-1}\sigma_1 + \dots + (-1)^{k-1} s_1\sigma_{k-1} + (-1)^k k\sigma_k = 0 & \text{при } k \leq n. \end{cases}$$

11*. Пусть p_k — симметрический многочлен от n переменных степени k , и многочлены $p_1, \dots, p_n$ алгебраически независимы, т. е. не существует ненулевого многочлена $Q(x_1, \dots, x_n)$ такого, что

$$Q(p_1, \dots, p_n) = 0.$$

Докажите, что любой симметрический многочлен от n переменных выражается через многочлены $p_1, \dots, p_n$.

12. Докажите, что множество симметрических многочленов образует подкольцо в кольце $K[x_1, \dots, x_n]$.

13. Многочлен называется *кососимметрическим* (или *антисимметрическим*), если он меняет знак при любой транспозиции переменных. Проверьте, что кососимметрический многочлен меняет знак при нечетных и не меняет знак при четных перестановках переменных.

14. Докажите, что сумма и разность кососимметрических многочленов — кососимметрический многочлен, а произведение — симметрический многочлен.

15. Докажите, что любой многочлен от двух переменных представляется в виде суммы симметрического и кососимметрического многочленов, причем единственным образом.

16. Докажите, что многочлен

$$D(x_1, \dots, x_n) = \prod_{1 \leq i < j \leq n} (x_i - x_j)$$

— кососимметрический.

17. Докажите, что любой кососимметрический многочлен представим в виде произведения $D(x_1, \dots, x_n)$ на симметрический многочлен.

18*. Докажите, что отображение

$$f(x_1, \dots, x_n) \rightarrow \sum_{\alpha \in S_n} f_{\alpha}(x_1, \dots, x_n)$$

переводит любой многочлен в симметрический, а отображение

$$f(x_1, \dots, x_n) \rightarrow \sum_{\alpha \in S_n} \varepsilon(\alpha) f_{\alpha}(x_1, \dots, x_n)$$

(где $\varepsilon(\alpha)$ — знак перестановки α) — в кососимметрический.

19*. Докажите, что если многочлен не меняется при четных перестановках, то его можно представить как сумму симметрического и кососимметрического многочленов.

§ 3.11. Быстрое умножение

Первым придумал быстрый алгоритм умножения в 1962 г. А. А. Карацуба*.

* Тогда он был аспирантом мехмата. В 1963–64 гг. преподавал в ФМШ № 18 при МГУ. Более 30 лет является профессором мехмата МГУ. Выдающийся специалист по аналитической теории чисел.

Идею его метода можно пояснить на следующем примере. Пусть перемножаются восьмизначные числа $U = \overline{u_1 \dots u_8}$ и $V = \overline{v_1 \dots v_8}$. Представим их как двузначные числа в 10^4 -значной системе счисления: $U = U_1 U_2$, $V = V_1 V_2$. Тогда их произведение можно представить в следующем виде:

$$UV = U_1 V_1 10^8 + ((U_1 - U_2)(V_2 - V_1) + U_1 V_1 + U_2 V_2) 10^4 + U_2 V_2.$$

Эта формула сводит умножение 8-значных чисел к трем операциям умножения и шести операциям сложения-вычитания 4-значных чисел (с учетом переносов в следующие разряды). Обычный способ требует четырех умножений и трех сложений-вычитаний, но так как три раза сложить 4-значные числа можно быстрее, чем один раз перемножить, то метод Карацубы уже 8-значные числа перемножает быстрее. В общем случае он требует для перемножения n -значных чисел по порядку не больше

$$n^{\log_2 3} < n^{1,585}$$

операций над цифрами, для школьного же метода требуется по порядку n^2 операций.

Рассмотрим вопрос о сложности умножения более подробно. Начнем с умножения многочленов.

Лемма 23. *Умножение двух многочленов степеней, меньших $2n$, можно свести к умножению трех пар многочленов степеней, меньших n , и сложению четырех пар многочленов степеней, меньших n , и вычитанию двух пар многочленов степеней, меньших $2n$, с помощью тождества*

$$\begin{aligned} (f_1 x^n + f_0)(g_1 x^n + g_0) = \\ = f_1 g_1 x^{2n} + ((f_1 + f_0)(g_1 + g_0) - f_1 g_1 - f_0 g_0) x^n + f_0 g_0. \end{aligned}$$

Обозначим через $M(n)$ наименьшее количество операций сложения, вычитания и умножения (выполняемых над коэффициентами многочленов и промежуточными числовыми результатами), требующихся для перемножения двух многочленов степеней, меньших n .

Лемма 24. *Справедливы неравенства*

$$M(n) \leq 2M(\lceil n/2 \rceil) + M(\lfloor n/2 \rfloor) + 4\lfloor n/2 \rfloor + 2n - 4.$$

Доказательство. Применим равенство

$$\begin{aligned} (f_1 x^{\lfloor n/2 \rfloor} + f_0)(g_1 x^{\lfloor n/2 \rfloor} + g_0) = \\ = f_1 g_1 x^{2\lfloor n/2 \rfloor} + ((f_1 + f_0)(g_1 + g_0) - f_1 g_1 - f_0 g_0) x^{\lfloor n/2 \rfloor} + f_0 g_0, \end{aligned}$$

где степени многочленов f_1 и g_1 меньше $\lceil n/2 \rceil$, а степени многочленов f_0 и g_0 меньше $\lfloor n/2 \rfloor$, и заметим, что для вычисления произведений $f_1 g_1$, $f_0 g_0$ требуется не более $M(\lceil n/2 \rceil) + M(\lfloor n/2 \rfloor)$ операций, для вычисления сумм $f_1 + f_0$, $g_1 + g_0$, $f_1 g_1 + f_0 g_0$ нужно не более $2\lfloor n/2 \rfloor + 2\lceil n/2 \rceil - 1$ операций (так как число операций равно наименьшему из количеств ненулевых коэффициентов у складываемых многочленов), для вычисления произведения $(f_1 + f_0)(g_1 + g_0)$ используется не более $M(\lceil n/2 \rceil)$ операций, для вычисления разности $(f_1 + f_0)(g_1 + g_0) - f_1 g_1 - f_0 g_0$ достаточно $n - 1$ операция, так как

$$(f_1 + f_0)(g_1 + g_0) - f_1 g_1 - f_0 g_0 = f_1 g_0 + f_0 g_1,$$

значит, степень этого многочлена равна $\lfloor n/2 \rfloor + \lceil n/2 \rceil - 2 = n - 2$, сложение многочленов $f_0 g_0$ и $f_1 g_1 x^{2\lfloor n/2 \rfloor}$ выполняется «бесплатно», так как они не имеют подобных членов, причем в их сумме отсутствует член вида $x^{2\lfloor n/2 \rfloor - 1}$, поэтому для сложения многочленов

$$f_0 g_0 + f_1 g_1 x^{2\lfloor n/2 \rfloor}, \quad (f_1 g_0 + f_0 g_1) x^{\lfloor n/2 \rfloor}$$

достаточно $n - 2$ операции. В итоге требуется дополнительно $4\lfloor n/2 \rfloor + 2n - 4$ операции. $\square$

Теорема 91. Если 2^k делит n , то справедливо неравенство

$$M(n) \leq 3^k (M(n/2^k) + 8n/2^k - 2) - 8n + 2,$$

а при любом n — неравенство

$$M(n) < (35/3)n^{\lg_2 3}.$$

Доказательство. Пусть $2^k m = n$. Тогда неравенство

$$M(n) \leq 3^k (M(m) + 8m - 2) - 8n + 2$$

доказывается индукцией по k . База ($k = 1$) доказана в лемме 2. Шаг индукции обосновывается тем же неравенством.

Выберем k так, чтобы $2^k < n \leq 2^{k+1}$. Тогда если $3 \cdot 2^{k-1} < n$, то

$$M(n) \leq M(2^{k+1}) < 3^{k-1} (M(4) + 30) \leq 3^{k-1} \cdot 55 < 55 \cdot \left(\frac{n}{3}\right)^{\lg_2 3} < \frac{35}{3} n^{\lg_2 3}.$$

Если же $n \leq 3 \cdot 2^{k-1}$, то

$$M(n) \leq M(3 \cdot 2^{k-1}) < 3^{k-1} (M(3) + 22) \leq 3^{k-1} \cdot 35 \leq (35/3)n^{\lg_2 3}. \quad \square$$

Перейдем к умножению чисел.

Пусть теперь $M(n)$ обозначает наименьшее количество операций сложения, вычитания и умножения, выполняемых над числами, меньшими a , требующихся для перемножения двух n -значных чисел, записанных в позиционной системе счисления по основанию a .

Лемма 25. *Справедливы неравенства*

$$M(2n) \leq 3M(n) + 19n, \quad M(2n+1) \leq 2M(n+1) + M(n) + 17n + 10.$$

Доказательство. Применим тождества

$$\begin{aligned} (f_1 b^{\lceil n/2 \rceil} + f_0)(g_1 b^{\lceil n/2 \rceil} + g_0) = \\ = f_1 g_1 b^{2\lceil n/2 \rceil} + (f_1 g_1 + f_0 g_0 - (f_1 - f_0)(g_1 - g_0))b^{\lceil n/2 \rceil} + f_0 g_0, \end{aligned}$$

где числа f_1 и $g_1 - \lfloor n/2 \rfloor$ -разрядные, а числа f_0 и g_0 соответственно $\lceil n/2 \rceil$ -разрядные, и заметим, что для вычисления произведений $f_1 g_1$ и $f_0 g_0$ требуется $M(\lceil n/2 \rceil) + M(\lfloor n/2 \rfloor)$ операций, для вычисления разностей и суммы $f_0 - f_1$, $g_0 - g_1$, $f_1 g_1 + f_0 g_0$ требуется не более

$$\begin{aligned} n(1 + \lfloor n/2 \rfloor - \lceil n/2 \rceil) + 2(\lfloor n/2 \rfloor + \lceil n/2 \rceil - 1) + 2(\lfloor n/2 \rfloor + \lceil n/2 \rceil) - 1 = \\ = 4n - 3 + n(1 + \lfloor n/2 \rfloor - \lceil n/2 \rceil) \end{aligned}$$

операций, так как числа $f_1 g_1$ и $f_0 g_0$ имеют не более чем $2\lfloor n/2 \rfloor$ и $2\lceil n/2 \rceil$ разрядов соответственно, а в случае четного n нужно еще $2\lfloor n/2 \rfloor = n$ операций для предварительного сравнения чисел (чтобы не вычитать из меньшего большее). Заметим далее, что для вычисления произведения $(f_1 - f_0)(g_1 - g_0)$ требуется не более $M(\lceil n/2 \rceil) + 1$ операций (одна операция для вычисления знака у произведения), для вычисления разности

$$f_1 g_1 + f_0 g_0 - (f_1 - f_0)(g_1 - g_0) = f_1 g_0 + f_0 g_1$$

требуется не более $2\lceil n/2 \rceil + 1 + 2\lceil n/2 \rceil - 1 = 4\lceil n/2 \rceil$ операций, сложение чисел $f_0 g_0$ и $f_1 g_1 b^{2\lceil n/2 \rceil}$ осуществляется «бесплатно» (записи этих чисел просто объединяются в одну запись), а для сложения чисел $f_1 g_1 b^{2\lceil n/2 \rceil} + f_0 g_0$ и $(f_1 g_0 + f_0 g_1)b^{\lceil n/2 \rceil}$ требуется не более $2n - \lceil n/2 \rceil + n + 1 - 1 = 2n + \lfloor n/2 \rfloor$ операций (так как число $f_1 g_0 + f_0 g_1$ имеет не более $n + 1$ разряда, а младшие $\lfloor n/2 \rfloor$ разрядов числа $f_0 g_0$ не участвуют в операциях). В итоге требуется дополнительно

$$\begin{aligned} 4n - 3 + n(1 + \lfloor n/2 \rfloor - \lceil n/2 \rceil) + 1 + 4\lceil n/2 \rceil + 2n + \lfloor n/2 \rfloor = \\ = 7n + 3\lceil n/2 \rceil + n(1 + \lfloor n/2 \rfloor - \lceil n/2 \rceil) - 2 \end{aligned}$$

операций. $\square$

Задачи и упражнения к § 3.11

В следующем цикле задач речь идет о том, как по возможности быстрее производить арифметические операции с дробями, сводя их к операциям над целыми числами (или многочленами).

1. Допустим, что дроби a/b и c/d несократимы. Пусть $(a, d) = g_1$, $(b, c) = g_2$. Докажите, что

$$((a/g_1)(c/g_2), (d/g_1)(b/g_2)) = 1.$$

2. Допустим, что дроби a/b и c/d несократимы и числа a, b, c, d меньше 10^n . Предложите способ умножения и деления этих дробей, в котором все промежуточные результаты будут меньше 10^n , если в окончательном ответе числитель и знаменатель меньше 10^n .

3. Пусть $(a, b) = (c, d) = 1$, $(b, d) = g_1$, $t = ad/g_1 + bc/g_1$, $(t, g_1) = g_2$. Докажите, что

$$(d/g_1, b/g_1) = (t, d/g_1) = (t, b/g_1) = 1,$$

$$g_2 = (t, g_1) = (t, (d/g_1)(b/g_1)g_1) = (t, bd/g_1),$$

$(g_2, d/g_1) = 1$, b делится на g_2 и

$$(t/g_2, (d/g_1)(b/g_2)) = 1.$$

4. Допустим, что дроби a/b и c/d несократимы и числа a, b, c, d меньше 10^n . Предложите способ сложения и вычитания этих дробей, в котором все промежуточные результаты будут меньше 10^n , кроме одного, который будет меньше 10^{2n} , если в окончательном ответе числитель и знаменатель меньше 10^n .

Отметим, что утверждения этих задач можно перенести и на многочлены.

5. Проверьте, что обычный способ умножения многочленов дает оценку

$$M(n) \leq M_s(n) = n^2 + (n-1)^2.$$

6. Для умножения многочленов найдите наименьшее n , при котором

$$M(n) < M_s(n).$$

7. Докажите, что сложение двух n -значных чисел можно выполнить за $2n-1$ операцию, вычитание меньшего из большего — за $3n-1$ операцию, вычитание с определением знака разности — за $4n-1$ операцию, а сложение $(n+m)$ -значного числа с n -значным можно выполнить за $2n+m-1$ операцию.

8. Докажите, что обычный способ умножения чисел дает оценку

$$M(n) < 5n^2.$$

Обозначим через $K(n)$ сложность возведения n -разрядного числа в квадрат и такое же обозначение будем использовать для сложности возведения в квадрат многочлена степени $n-1$.

9. Используя тождество

$$ab = \frac{(a+b)^2 - (a-b)^2}{4},$$

докажите для случая операций с числами неравенство

$$M(n) \leq 2K(n) + 13n + O(1),$$

а для случая операций с многочленами — неравенство

$$M(n) \leq 2K(n) + 6n + 4.$$

§ 3.12. Разложение на бесквадратные множители

Для многочленов над произвольным полем дадим следующее

Определение 91. Разложение многочлена

$$P = q_1 q_2^2 \dots q_k^k$$

такое, что сомножители q_i не имеют кратных корней и попарно взаимно просты, называется *бесквадратной факторизацией первого типа* многочлена P .

Обозначим

$$Q_i = q_i q_{i+1} \dots q_k,$$

тогда

$$P = Q_1 \dots Q_k, \quad Q_i \mid Q_{i+1}, \quad i = 1, \dots, k-1,$$

и многочлены Q_i не имеют кратных корней. Такую факторизацию назовем *бесквадратной факторизацией второго типа*.

Упражнение 81. Проверьте, что оба типа бесквадратной факторизации однозначно восстанавливаются один по другому с помощью формул

$$q_i = Q_i / Q_{i+1}, \quad Q_i = P_i / P_{i+1}, \quad P_i = q_i q_{i+1}^2 \dots q_k^{k-i+1}.$$

Пусть $P = q_1 q_2^2 \dots q_k^k$, — бесквадратная факторизация первого типа. Следующая лемма справедлива для многочленов над любым полем нулевой характеристики. Производную многочлена P обозначаем $\frac{dP}{dx}$.

Лемма 26. Для последовательности многочленов P_i , начинающейся с $P_1 = P$ и определяемой равенствами $P_{i+1} = \left(P_i, \frac{dP_i}{dx}\right)$, справедливо тождество

$$P_i = q_i q_{i+1}^2 \dots q_k^{k-i+1} = Q_i Q_{i+1} \dots Q_k \quad (i = 1, \dots, k),$$

где $Q_i = q_i q_{i+1} \dots q_k$, откуда

$$Q_i = \frac{P_i}{P_{i+1}}, \quad q_i = \frac{Q_i}{Q_{i+1}} \quad (i = 1, \dots, k),$$

и таким образом оба вида факторизации существуют и определены однозначно.

Доказательство. Согласно предположению индукции и формуле Лейбница

$$\begin{aligned} \frac{dP_i}{dx} &= \frac{dq_i}{dx} q_{i+1}^2 \dots q_k^{k-i+1} + q_i 2q_{i+1} \frac{dq_{i+1}}{dx} \dots q_k^{k-i+1} + \dots \\ &\quad \dots + q_i q_{i+1}^2 \dots q_{k-1}^{k-i} (k-i+1) q_k^{k-i} \frac{dq_k}{dx} = \\ &= P_{i+1} \left(\frac{dq_i}{dx} q_{i+1} \dots q_k + \dots + q_i q_{i+1} \dots q_{k-1} (k-i+1) \frac{dq_k}{dx} \right). \end{aligned}$$

Сумма, стоящая в скобках, взаимно проста с q_i , потому что все слагаемые, кроме первого, кратны q_i , а первое слагаемое взаимно просто с ним. Действительно все его сомножители взаимно просты с q_i , так как q_i взаимно просты друг с другом и не имеют кратных корней, поэтому

$$\left(q_i, \frac{dq_i}{dx} \right) = 1.$$

Аналогичным образом проверяем, что сумма, стоящая в скобках, взаимно проста с $q_{i+1}, \dots, q_k$, а значит, и с произведением $Q_i = q_i q_{i+1} \dots q_k$. Поэтому

$$\left(\frac{dP_i}{dx}, P_i \right) = P_{i+1} \left(\frac{dP_i}{dx} / P_i, Q_i \right) = P_{i+1},$$

чем и доказан шаг индукции. $\square$

В стандартном алгоритме бесквадратной факторизации рекуррентно вычисляется последовательность многочленов по формулам $P_{i+1} = \left(P_i, \frac{dP_i}{dx} \right)$, где, как только что доказано,

$$P_i = q_i q_{i+1}^2 \dots q_k^{k-i+1} = Q_i Q_{i+1} \dots Q_k,$$

после чего находятся делением многочлены

$$Q_i = \frac{P_i}{P_{i+1}}, \quad q_i = \frac{Q_i}{Q_{i+1}}.$$

Изложим алгоритм Остроградского* бесквадратной факторизации в обозначениях самого Остроградского и оценим его сложность (т.е. число выполняемых им операций).

* Остроградский Михаил Васильевич (1801–1862) — выдающийся русский математик и механик. Один из основателей петербургской математической школы.

Пусть $P = P_1$ — факторизуемый многочлен, положим

$$P_2 = \left(P_1, \frac{dP_1}{dx} \right), \quad Q_1 = \frac{P_1}{P_2}, \quad R_1 = \frac{\frac{dP_1}{dx}}{P_2}, \quad q_1 = \left(Q_1, R_1 - \frac{dQ_1}{dx} \right),$$

$$Q_2 = \frac{Q_1}{q_1}, \quad R_2 = \frac{R_1 - \frac{dQ_1}{dx}}{q_1}, \quad q_2 = \left(Q_2, R_2 - \frac{dQ_2}{dx} \right)$$

и так далее, пока не получим $R_{k+1} = \frac{dQ_{k+1}}{dx}$. Тогда $P = q_1 q_2^2 \dots q_k^k$ — искомое разложение, потому что q_i не имеют кратных корней и взаимно просты. Отметим, что попутно найдено разложение $P = Q_1 Q_2 \dots Q_k$, где $Q_i = q_i \dots q_k$ ($i = 1, \dots, k$) тоже бесквадратные множители, но уже не взаимно простые, а последовательно делящие друг друга.

Обосновывается алгоритм Остроградского с помощью его замечательных тождеств.

Теорема 92 (Остроградский). *Для определенных выше последовательностей многочленов справедливы тождества*

$$R_{i+1} = \frac{\frac{dP_{i+1}}{dx}}{P_{i+2}} = \frac{R_i - \frac{dQ_i}{dx}}{q_i}, \quad q_i = \left(Q_i, R_i - \frac{dQ_i}{dx} \right).$$

Доказательство. Применяя индукцию, получаем, что

$$R_i - \frac{dQ_i}{dx} = \frac{\frac{dP_i}{dx}}{P_{i+1}} - \frac{d(P_i/P_{i+1})}{dx} = \frac{P_i \frac{dP_{i+1}}{dx}}{P_{i+1}^2} = \frac{Q_i \frac{dP_{i+1}}{dx}}{P_{i+1}} = \frac{Q_{i+1} q_i \frac{dP_{i+1}}{dx}}{P_{i+1}},$$

откуда имеем

$$R_{i+1} = \frac{R_i - \frac{dQ_i}{dx}}{q_i} = \frac{Q_{i+1} \frac{dP_{i+1}}{dx}}{P_{i+1}} = \frac{\frac{dP_{i+1}}{dx}}{P_{i+2}}.$$

Так как

$$P_i = q_i q_{i+1}^2 \dots q_k^{k-i+1}, \quad R_i = \frac{\frac{dP_i}{dx}}{P_{i+1}}, \quad Q_i = q_i \dots q_k,$$

из теоремы о понижении кратности корня при дифференцировании вытекает, что $(R_i, Q_i) = 1$, откуда следует уже безо всякой индукции, что

$$\begin{aligned} \left(Q_i, R_i - \frac{dQ_i}{dx} \right) &= (Q_i, R_{i+1} q_i) = (Q_{i+1} q_i, R_{i+1} q_i) = (Q_{i+1} q_i, R_{i+1} q_i) = \\ &= q_i (Q_{i+1}, R_{i+1}) = q_i. \end{aligned}$$

Заметим еще, что из формул

$$R_i = \frac{\frac{dP_i}{dx}}{P_{i+1}}, \quad Q_i = \frac{P_i}{P_{i+1}}$$

вытекает, что $\deg R_i = \deg P_i - \deg P_{i+1} - 1 = \deg Q_i - 1$. $\square$

Преимущество алгоритма Остроградского перед стандартным алгоритмом очевидно ввиду того, что на каждом шаге итерации он требует нахождения НОД многочленов меньшей степени, чем в стандартном алгоритме, и вместо двух делений использует только одно, причем для многочленов опять же меньшей степени. Кроме того, он допускает хорошую оценку сложности при использовании в нем быстрых алгоритмов умножения, деления и вычисления НОД.

Оценка сложности алгоритма Остроградского получается довольно просто, если воспользоваться следующим замечанием.

Пусть $M(n)$ — любая оценка сложности умножения двух многочленов степени n , удовлетворяющая условию супераддитивности: $M(x) + M(y) \leq M(x + y)$, и $G(n)$ — такая же оценка сложности вычисления НОД двух многочленов. Например, в качестве $M(n)$ можно взять $Cn^{\log_2 3}$, а в качестве $G(n)$ можно взять $CM(n) \lg n$ при большой константе C (это мы не будем доказывать).

Положим $\deg Q_i = n_i$, $\deg q_i = m_i$, $\deg P_2 = p = n_2 + \dots + n_k$, тогда $m_i = n_i - n_{i+1}$, $\deg R_i = n_i - 1$. Сложность деления без остатка многочлена степени m на многочлен степени n оценим как $3(M(m - n) + m - n) + M(m)$, значит, сложность деления двух разных многочленов степени не выше m на один и тот же многочлен степени n оценивается как $3(M(m - n) + m - n) + 2M(m)$, тогда нужная оценка имеет вид

$$\begin{aligned} n + G(n) + 3M(n - p) + 3n - 3p + 2M(n) + \sum_{i=1}^k (G(n_i) + 2M(n_i) + 2n_i) + \\ + \sum_{i=2}^k (3M(n_i) + 3n_i) \leq n + G(n) + 3(M(n - p) + n - p) + 2M(n) + \\ + G(n) + 2M(n) + 2n + 3(M(p) + p) \leq 2G(n) + 7M(n) + 6n. \end{aligned}$$

Полученная оценка показывает, что сложность алгоритма Остроградского бесквадратной факторизации многочлена степени n *асимптотически лишь в два раза* превосходит сложность алгоритма нахождения НОД двух многочленов степени n .

Интересно отметить, что Остроградский предложил еще один вариант алгоритма факторизации, основанный на тождестве $q_j = \left(Q, R - j \frac{dQ}{dx} \right)$,

где

$$Q = Q_1 = \frac{P_1}{P_2} = \frac{P}{P_2}, \quad R = R_1 = \frac{\frac{dP_1}{dx}}{\frac{dP_2}{dx}}, \quad P_2 = \left(\frac{dP_1}{dx}, P_1 \right).$$

Доказательство вытекает из цепочки равенств (в которой для краткости дифференцирование обозначается штрихом)

$$\begin{aligned} R &= \frac{(P_1)'}{P_2} = \frac{(q_1 q_2^2 \dots q_k^k)'}{q_2 \dots q_{k-1}^k} = \sum_{i=1}^k i q_1 \dots q_{i-1} (q_i)' q_{i+1} \dots q_k, \\ Q' &= \sum_{i=1}^k q_1 \dots q_{i-1} (q_i)' q_{i+1} \dots q_k, \\ R - jQ' &= \sum_{i=1}^k (i - j) q_1 \dots q_{i-1} (q_i)' q_{i+1} \dots q_k, \end{aligned}$$

обосновываемой правилом дифференцирования Лейбница, и замечания о том, что в последней сумме все слагаемые, кроме s -го, делятся на q_s , а оно взаимно просто с многочленом q_s (так как все его сомножители с ним взаимно просты), следовательно, $(R - jQ', q_s) = 1$ при $s \neq j$, и, очевидно, многочлен $R - jQ$ делится на многочлен q_j .

Указанные формулы Остроградского более элегантны, чем предыдущие, но сложность последнего алгоритма очевидно больше, чем предыдущего, так как в нем степени многочленов последовательности, у которых приходится вычислять НОД, не уменьшаются, и он не допускает очевидной хорошей верхней оценки. Однако если нужно вычислить не все множители q_i , а только любой один из них, то этот алгоритм, вероятно, является быстрее.

Задачи и упражнения к § 3.12

1. Обоснуйте стандартный алгоритм бесквадратной факторизации со всеми подробностями.
2. Обоснуйте второй алгоритм бесквадратной факторизации Остроградского со всеми подробностями.
3. Выполните бесквадратную факторизацию многочлена стандартным методом и методом Остроградского

$$x^{10} + 3x^9 - 5x^8 - 21x^7 + x^6 + 45x^5 + 17x^4 - 39x^3 - 22x^2 + 12x + 8$$

и найдите его корни.

4.** Докажите, что сложность деления без остатка многочлена степени m на многочлен степени n оценивается как

$$3(M(m-n) + m - n) + M(m).$$

5*. Докажите, что сложность деления двух разных многочленов степени не выше m на один и тот же многочлен степени n оценивается как

$$3(M(m-n) + m - n) + 2M(m).$$

6. Докажите, что сложность деления с остатком многочлена степени m на многочлен степени n со старшим коэффициентом 1 оценивается как $(m-n+1)(2n+1)$, а без остатка — как $(m-n)(2n+1)$.

7. Докажите, что обычный алгоритм Евклида для многочленов степени не выше n имеет оценку сложности

$$G(n) \leq \frac{7}{2}n^2 + \frac{3}{2}n.$$

У к а з а н и е. Надо учесть необходимость на каждом шаге алгоритма выполнять приведение полученного остатка к виду, в котором старший коэффициент будет равен единице.

8. Докажите, что обычный алгоритм Евклида для многочленов степени не выше n имеет оценку сложности $\frac{7}{2}(n^2 - m^2) + O(n)$, где m — степень вычисленного НОД.

9*. Докажите, что предыдущую оценку нельзя существенно улучшить, рассмотрев вычисление НОД(T_n, T_{n-1}), где T_n — многочлены Чебышёва.

10*. Докажите, что обычный алгоритм Евклида для многочленов степени n и m имеет оценку сложности $G(n) \leq 2nm + \frac{1}{2}m^2 + \frac{5}{2}n$.

У к а з а н и е. Сначала рассмотрите случай, когда на каждом шаге алгоритма степень уменьшается на единицу. Потом покажите, что в общем случае оценка не выше, чем в этом частном случае.

11. Докажите, что сложность деления с остатком n -разрядного числа на m -разрядное имеет оценку сложности $C(n-m)m$, где $C > 0$ — константа.

12*. Докажите, что обычный алгоритм Евклида для n -разрядных чисел имеет оценку сложности $G(n) \leq Cn^2$.

У к а з а н и е. Примените предыдущую задачу.

13. Докажите, что сложность вычисления последовательности многочленов Q_i, q_i по формулам $Q_i = P_i/P_{i+1}$, $q_i = Q_i/Q_{i+1}$ при известной последовательности P_i с помощью школьного алгоритма оценивается как $2(n^2 + n_1^2)$, где $n = \deg P = \deg P_1$, $n_1 = \deg Q_1$.

У к а з а н и е. Примените задачу 6.

14. Докажите, что сложность вычисления последовательности многочленов P_i стандартным алгоритмом по формулам

$$P_{i+1} = \left(P_i, \frac{dP_i}{dx} \right)$$

оценивается как $4n^2 + O(n)$.

У к а з а н и е. Примените задачу 8.

15. Докажите, что сложность стандартного алгоритма бесквадратной факторизации многочлена степени n оценивается как $8n^2 + O(n)$.

У к а з а н и е. Примените предыдущую задачу.

Глава IV. Алгебраические уравнения

§ 4.1. Решение кубических уравнений

Значительно сложнее, чем квадратное, решить кубическое уравнение

$$x^3 + ax^2 + bx + c = 0.$$

Оно было решено только в XVI в. итальянцами дель Ферро * и Тарталья.

Вкратце история этого замечательного открытия такова. Первым нашел решение в нескольких важных частных случаях профессор математики из Болоньи дель Ферро. Перед смертью под большим секретом он передал тайну своему близкому другу или родственнику Фиоре, который, будучи посредственным математиком, после этого легко выигрывал популярные в то время научные диспуты, предлагая оппонентам для решения задачи, сводящиеся к кубическим уравнениям.

Никколо Тарталья в детстве во время войны был сильно напуган и, кажется, ранен в лицо, и поэтому он вошел в историю не под своим именем, а под прозвищем Тарталья, в переводе означающим «заика». Азбуку он выучил под руководством учителя только до буквы «К» (на дальнейшее у матери не хватило денег), и все остальное ему пришлось постигать самоучкой. Повзрослев, он подрабатывал научным консультантом в Венецианском арсенале (и был одним из первых математиков-прикладников **). За неделю до диспута до него дошла молва, что оппонент владеет секретом решения кубических уравнений...

На диспуте Тарталья решил все предложенные ему задачи, а ошеломленный противник не сумел решить в ответ ни одной, даже основанной на известных ему случаях разрешимости, полученных в наследство от дель Ферро.

Тот вариант решения кубического уравнения, который мы сейчас изложим, принадлежит Гудде ***. Прежде всего, выделив полный куб,

* Ш. дель Ферро (Scipion del Ferro, 1465–1526) — итальянский математик. Нашел способ решения кубических уравнений типа $x^3 + mx = n$.

** Легенда гласит, что он первым объяснил артиллеристам, что для максимальной дальности орудия надо поднять его ствол под углом 45° .

*** И. Гудде (Johann Hudde, 1633–1704) — голландский математик. Открыл правило нахождения кратных корней.

избавимся от коэффициента при x^2 :

$$\begin{aligned}
 x^3 + ax^2 + bx + c &= \\
 &= x^3 + 3\frac{a}{3}x^2 + 3\left(\frac{a}{3}\right)^2 x + \left(\frac{a}{3}\right)^3 - 3\left(\frac{a}{3}\right)^2 x - \left(\frac{a}{3}\right)^3 + bx + c = \\
 &= \left(x + \frac{a}{3}\right)^3 + \left(b - \frac{a^2}{3}\right)x + c - \left(\frac{a}{3}\right)^3 = \\
 &= \left(x + \frac{a}{3}\right)^3 + \left(b - \frac{a^2}{3}\right)\left(x + \frac{a}{3}\right) - \frac{a}{3}\left(b - \frac{a^2}{3}\right) + c - \left(\frac{a}{3}\right)^3 = \\
 &= \left(x + \frac{a}{3}\right)^3 + A\left(x + \frac{a}{3}\right) + B.
 \end{aligned}$$

В переписанном таким образом уравнении в качестве неизвестного удобно рассматривать $x + a/3$. После нахождения корней уравнения $x^3 + Ax + B$, вычтем из них $a/3$ и получим корни исходного уравнения.

Самый простой путь к решению уравнения третьей степени $x^3 + Ax + B$ состоит в следующем. Будем искать решение в виде суммы *двух слагаемых* (!!!) $x = u + v$, на которые потом наложим некоторые условия.

Подставим $x = u + v$ в уравнение:

$$\begin{aligned}
 0 &= (u + v)^3 + A(u + v) + B = u^3 + v^3 + 3uv(u + v) + A(u + v) + B = \\
 &= (u^3 + v^3 + B) + (u + v)(3uv + A).
 \end{aligned}$$

Пусть и первое, и второе слагаемые по отдельности равны нулю:

$$\begin{cases} u^3 + v^3 + B = 0; \\ (u + v)(3uv + A) = 0. \end{cases}$$

Заметим, что если $B \neq 0$, то $x = 0$ не является корнем уравнения (при $B = 0$ уравнение становится тривиальным). Значит, $x = u + v \neq 0$, и, упрощая второе уравнение, приходим к системе

$$\begin{cases} u^3 + v^3 = -B; \\ 3uv = -A. \end{cases} \quad (*)$$

Эта система легко решается. Выразим из второго уравнения переменную v через u формулой $v = -A/(3u)$, и подставим ее в первое уравнение:

$$u^3 - \frac{A^3}{27u^3} = -B.$$

Получаем квадратное относительно неизвестного u^3 уравнение

$$(u^3)^2 + Bu^3 - \frac{A^3}{27} = 0.$$

Формулы для квадратного уравнения дают решение

$$u^3 = -\frac{B}{2} \pm \sqrt{\frac{A^3}{27} + \frac{B^2}{4}},$$

откуда

$$v^3 = -\frac{A^3}{27\left(-\frac{B}{2} \pm \sqrt{\frac{A^3}{27} + \frac{B^2}{4}}\right)} = -\frac{B}{2} \mp \sqrt{\frac{A^3}{27} + \frac{B^2}{4}}.$$

Отметим, что при $\frac{A^3}{27} + \frac{B^2}{4} < 0$ квадратное уравнение не имеет решений.

При $\frac{A^3}{27} + \frac{B^2}{4} \geq 0$ исходное кубическое уравнение имеет решение

$$x_1 = u_1 + v_1 = \sqrt[3]{-\frac{B}{2} + \sqrt{\frac{A^3}{27} + \frac{B^2}{4}}} + \sqrt[3]{-\frac{B}{2} - \sqrt{\frac{A^3}{27} + \frac{B^2}{4}}},$$

где радикал $\sqrt[3]{}$ означает единственный неотрицательный вещественный корень третьей степени из вещественного числа. Выведенная формула называется (исторически не совсем справедливо) формулой Кардано *.

Несложно показать, что при $\frac{A^3}{27} + \frac{B^2}{4} > 0$ других вещественных решений нет. Для доказательства рассмотрим график функции $y = x^3 + Ax = x(x^2 + A)$. Вещественные корни уравнения $x^3 + Ax + B = 0$ суть абсциссы точек пересечения этого графика с горизонтальной прямой $y = -B$. При $A \geq 0$ функция $y = x^3 + Ax$ возрастает (так как производная $y'(x) = 3x^2 + A > 0$).

Значит, при $A \geq 0$ и при любом B прямая $y = -B$ пересекает график $y = x^3 + Ax$ в одной точке, т. е. есть только один вещественный корень (рис. 22).

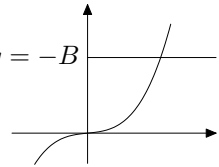


Рис. 22

При $A < 0$ график функции $y = x^3 + Ax$ имеет вид, изображенный на рис. 23.

Исходное уравнение имеет ровно три решения при B , находящемся между локальным минимумом $y_{\min}$ и локальным максимумом $y_{\max}$ этой функции. Найдем эти уравнения. Так как

$$y'(x) = 3x^2 + A = 0,$$

* В честь Дж. Кардано (Girolamo Cardano, 1501–1576), итальянского врача, астролога, оккультиста, математика и изобретателя, впервые ее опубликовавшего. По преданию покончил с собой, чтобы исполнился им самим составленный гороскоп.

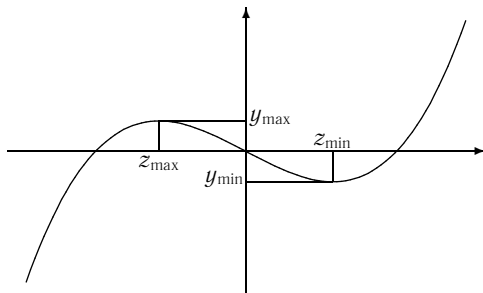


Рис. 23

то экстремальные точки $x = \pm \sqrt{-\frac{A}{3}}$, а экстремальные значения

$$y_{\min} = y \sqrt{-\frac{A}{3}} = \frac{2}{3} A \sqrt{-\frac{A}{3}}, \quad y_{\max} = y \left(-\sqrt{-\frac{A}{3}} \right) = -\frac{2}{3} A \sqrt{-\frac{A}{3}}.$$

Значит, в точности при

$$\frac{2}{3} A \sqrt{-\frac{A}{3}} < B < -\frac{2}{3} A \sqrt{-\frac{A}{3}}, \quad A < 0$$

либо при $A \geq 0$ уравнение третьей степени имеет единственный вещественный корень. Заметим, что эти условия эквивалентны единственному условию $\frac{A^3}{27} + \frac{B^2}{4} > 0$.

Задачи и упражнения к § 4.1

1. Если все корни уравнения $x^3 + px + q = 0$ действительны, то $p < 0$.
2. Используя формулу Кардано—Ферро—Тартальи, решите уравнения: а) $x^3 + 3x^2 - 3x - 14 = 0$; б) $x^3 - 12x + 16 = 0$.
3. Найдите сумму кубов всех корней уравнения $ax^3 + bx^2 + cx + d = 0$.
4. Пусть a, b, c — корни уравнения $x^3 + px + q = 0$. Напишите уравнение, корнями которого будут числа

$$\frac{b+c}{a^2}, \quad \frac{a+c}{b^2}, \quad \frac{b+a}{c^2}.$$

5. Докажите, что с помощью подстановки $x = y + a$ можно свести любое уравнение n -й степени к уравнению с нулевым коэффициентом при x^{n-1} .

6. Пусть уравнение $a_n x^n + \dots + a_0 = 0$ имеет корни x_i , $i = 1, \dots, n$. Решите уравнения

а) $a_n x^n - a_{n-1} x^{n-1} + a_{n-2} x^{n-2} - \dots \mp a_0 = 0$;

б) $a_0 x^n + \dots + a_n = 0$;

в) $a_n x^n + a_{n-1} b x^{n-1} + \dots + a_0 b^n = 0$.

7. С помощью замены переменных $x = u + v$ решите, подобно кубическому, уравнение Муавра $x^5 - 5ax^3 + 5a^2x - 2b = 0$.

8. При каких a , b , c корни уравнения $x^3 + ax^2 + bx + c = 0$ образуют

а) арифметическую;

б) геометрическую прогрессию?

§ 4.2. Неприводимый случай

Как следует из исследования, проведенного в предыдущем пункте, при

$$\frac{A^3}{27} + \frac{B^2}{4} < 0$$

уравнение $x^3 + Ax + B = 0$ имеет ровно три действительных решения. Однако можно показать, что найти эти решения с помощью четырех правил арифметики и извлечения арифметических корней произвольных степеней невозможно. Поэтому первооткрыватели формул для решения уравнения третьей степени старательно обходили этот так называемый неприводимый случай уравнения третьей степени.

В конце XVI в. Виет сделал открытие, позволившее ему решить это уравнение в неприводимом случае в тригонометрических функциях. Он обратил внимание на то, что формула косинуса тройного аргумента имеет вид некоторого уравнения третьей степени:

$$\cos 3\varphi = 4 \cos^3 \varphi - 3 \cos \varphi.$$

Упражнение 82. Докажите эту формулу.

Можно попытаться свести уравнение третьей степени $x^3 + Ax + B = 0$ к виду $4x^3 - 3x = C$ заменой переменной. Это достигается уже простейшей заменой вида $x = kt$:

$$x^3 + Ax + B = 0 \iff k^3 t^3 + A k t + B = 0.$$

Потребуем, чтобы коэффициент при t^3 относился к коэффициенту при t как 4 к -3, т. е.

$$\frac{k^3}{Ak} = \frac{4}{-3},$$

откуда

$$k = \pm \sqrt{-\frac{4A}{3}}$$

(заметим, что A меньше нуля). Уравнение перепишем в виде

$$-\frac{4A}{3}\sqrt{-\frac{4A}{3}}t^3 + A\sqrt{-\frac{4A}{3}}t + B = 0,$$

или, что равносильно,

$$4t^3 - 3t = \frac{3\sqrt{3}B}{2A\sqrt{-A}} = C.$$

Заметим, что

$$|C| < 1 \iff \frac{A^3}{27} + \frac{B^2}{4} < 0.$$

Положив $t = \cos \varphi$, имеем

$$\cos 3\varphi = 4 \cos^3 \varphi - 3 \cos \varphi = C,$$

значит,

$$\varphi = \pm \arccos C + \frac{2\pi n}{3}, \quad n \in \mathbb{Z}.$$

Отсюда находим три значения для t

$$t_1 = \cos\left(\frac{1}{3} \arccos C\right), \quad t_2 = \cos\left(\frac{1}{3} \arccos C + \frac{2}{3}\pi\right),$$

$$t_3 = \cos\left(\frac{1}{3} \arccos C - \frac{2}{3}\pi\right),$$

и, соответственно, три вещественных корня уравнения $x^3 + Ax + B = 0$ при

$$\frac{A^3}{27} + \frac{B^2}{4} < 0$$

равны

$$x_1 = \sqrt{-\frac{A}{3}} \cos\left(\frac{1}{3} \arccos \frac{3\sqrt{3}B}{2A\sqrt{-A}}\right),$$

$$x_2 = -\sqrt{-\frac{A}{3}} \cos\left(\frac{1}{3} \arccos \frac{3\sqrt{3}B}{2A\sqrt{-A}}\right) - \sqrt{-A} \sin\left(\frac{1}{3} \arccos \frac{3\sqrt{3}B}{2A\sqrt{-A}}\right),$$

$$x_3 = -\sqrt{-\frac{A}{3}} \cos\left(\frac{1}{3} \arccos \frac{3\sqrt{3}B}{2A\sqrt{-A}}\right) + \sqrt{-A} \sin\left(\frac{1}{3} \arccos \frac{3\sqrt{3}B}{2A\sqrt{-A}}\right).$$

Задачи и упражнения к § 4.2

1. Решите уравнение $x^3 - 19x + 30 = 0$ «угадыванием» корней и убедитесь в том, что это неприводимый случай. Найдите тригонометрическое решение методом Виета.

2. Является ли число $\sqrt[3]{\sqrt{5}+2} - \sqrt[3]{\sqrt{5}-2}$ рациональным?

3. Решите неприводимый случай, используя формулу синуса тройного угла.

4. Решите уравнение $x^3 - 3(a^2 + 1)x - 2a(a^2 + 1) = 0$, используя формулу тангенса тройного угла.

5. Решите по формуле Кардано уравнения

а) $x^3 - 3abx + a^3 + b^3 = 0$;

б) $x^3 - 3abcdx + c^2da^3 + cd^2b^3 = 0$.

6*. Многочлен $f(x)$ таков, что для любого достаточно большого $n \in \mathbb{N}$ уравнение $f(x) = n$ имеет рациональные корни. Докажите, что его степень равна 1.

7. Найдите рациональные корни многочленов

а) $x^5 + x^4 - 6x^3 - 14x^2 - 11x - 3$;

б) $x^6 - 6x^5 + 11x^4 - x^3 - 18x^2 + 20x - 8$;

в) $24x^5 + 10x^4 - x^3 - 19x^2 - 5x + 6$.

8. Многочлен $f(x)$ с целыми коэффициентами не имеет целых корней, если $f(0)$ и $f(1)$ — нечетные числа.

9. Многочлен $f(x)$ с целыми коэффициентами не имеет рациональных корней, если $f(x_1) = \pm 1$, $f(x_2) = \pm 1$ при $x_1, x_2 \in \mathbb{Z}$, $|x_1 - x_2| > 2$. Если же $|x_1 - x_2| \leq 2$, то рациональным корнем может быть только $(x_1 + x_2)/2$.

10*. Докажите, что $\cos 2\pi/7$ является корнем уравнения $8x^3 + 4x^2 - 4x - 1 = 0$. Докажите, что это число иррациональное.

11. Убедитесь, что для предыдущего уравнения методом Кардано получается неприводимый случай, а его тригонометрическое решение трудно идентифицируется с указанным выше.

§ 4.3. Комплексные числа

Формулы для решения уравнения $x^3 + Ax + B = 0$ из предыдущих параграфов имеют совершенно различный вид: в одном случае используются алгебраические, в другом тригонометрические выражения. Тем не менее, решение этого уравнения, предложенное в предыдущем параграфе, можно довести до конца и в неприводимом случае. Для этого необходимо придать смысл понятию решения квадратного уравнения с отрицательным дискриминантом. Мы споткнулись именно на квадратном относительно u^3 уравнении:

$$(u^3)^2 + Bu^3 - \frac{A^3}{27} = 0.$$

Однако решение таких уравнений эквивалентно извлечению квадратного корня из отрицательного числа. В самом деле, всякое квадратное уравнение эквивалентно уравнению вида $x^2 = c$ (достаточно выделить полный квадрат). Если $c < 0$, то положим решениями уравнения $x^2 = c$ два

чисто мнимых числа $x_1 = \sqrt{|c|}i$, $x_2 = -\sqrt{|c|}i$, т. е. $\sqrt{c} = \pm\sqrt{|c|}i$. Здесь число i — мнимая единица — обладает свойством $i^2 = i \cdot i = -1$, т. е. является одним из решений квадратного уравнения $x^2 = -1$ (другим решением должно быть число $-i$). Чтобы рассматривать решения произвольных квадратных уравнений с отрицательным дискриминантом, нужно ввести в рассмотрение суммы вида $z = a + bi$, где a и b — действительные числа. Действительно, мы перешли от произвольного квадратного уравнения к уравнению $x^2 = c$ при помощи замены переменной $x' = x + d$, где d — действительное число.

Оказывается, что для выражений вида $z = a + bi$, называемых *комплексными числами*, можно построить свою арифметику.

Определение 92. Определим сложение и умножение комплексных чисел z_1, z_2 следующими формулами:

$$\begin{aligned} z_1 + z_2 &= (a_1 + b_1i) + (a_2 + b_2i) = (a_1 + a_2) + (b_1 + b_2)i, \\ z_1 \cdot z_2 &= (a_1 + b_1i)(a_2 + b_2i) = a_1a_2 - b_1b_2 + (a_1b_2 + a_2b_1)i, \end{aligned}$$

где a_1, a_2, b_1, b_2 — действительные числа.

Заметим, что при сложении мы почленно складываем «действительные» части $a_1 + a_2$ и «мнимые» части $b_1 + b_2$. При умножении мы раскрываем скобки и, как обычно, перемножаем члены, пользуясь только свойством мнимой единицы $i \cdot i = -1$.

Примеры. 1. $(1 + i) + (2 - 3i) = 3 - 2i$.

2. $(1 + i) + (-1 - i) = 0$.

3. $(1 + i)(1 - i) = 1 - i^2 = 2$.

Определение 93. У комплексного числа $z = a + bi$ число a называется *действительной частью* и обозначается $\operatorname{Re} z$, а число b называется *мнимой частью* и обозначается $\operatorname{Im} z$.

Примеры. 1. $\operatorname{Re}(1 + i) = 1$.

2. $\operatorname{Im}(1 - i) = -1$.

Упражнение 83. Проверьте тождество $\operatorname{Re}(iz) = -\operatorname{Im} z$.

Очевидно, что для любого комплексного числа $z = a + bi$ есть противоположное $-z = -a - bi$: $z + (-z) = 0 + 0i = 0$.

Менее очевидно, что для $z \neq 0$ есть обратное число (относительно умножения)

$$z^{-1} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}i.$$

Упражнение 84. Проверьте, что $z \cdot z^{-1} = 1 + 0i = 1$.

Примеры. 1. $(3 + 4i)^{-1} = \frac{3}{25} - \frac{4}{25}i$.

2. $(1 + i)^{-1} = \frac{1}{2} - \frac{1}{2}i$.

Определение 94. Обозначим через $|z|$ неотрицательное действительное число

$$\sqrt{\operatorname{Re} z^2 + \operatorname{Im} z^2} = \sqrt{a^2 + b^2},$$

называемое *модулем* комплексного числа z . Через $\bar{z}$ обозначим комплексное число $\operatorname{Re} z - i \operatorname{Im} z = a - ib$, называемое *сопряженным* к z комплексным числом.

Примеры. 1. $|3 + 4i| = \sqrt{3^2 + 4^2} = 5$.

2. $\overline{3 + 4i} = 3 - 4i$.

Упражнение 85. Проверьте, что

$$z^{-1} = \frac{\bar{z}}{|z|^2}, \quad |\bar{z}| = |z|, \quad z + \bar{z} = 2a, \quad |z^{-1}| = \frac{1}{|z|}, \quad |z|^2 = z \cdot \bar{z}.$$

Проверьте, что уравнение $z_2 w = z_1$ с комплексной неизвестной w при $z_2 \neq 0$ имеет единственное решение $w = z_1 \cdot z_2^{-1}$. Найдите это решение непосредственно.

Определение 95. Число $z_1 \cdot z_2^{-1}$ называется *частным* чисел z_1, z_2 и обозначается $\frac{z_1}{z_2}$.

Примеры. 1. $\frac{1}{(3 - 4i)} = \frac{3}{25} + \frac{4}{25}i$.

2. $\frac{(3 + 4i)}{(3 - 4i)} = (3 + 4i) \left(\frac{3}{25} + \frac{4}{25}i \right) = -\frac{7}{25} + \frac{24}{25}i$.

3. Если $|z| = 1$, то $\frac{1}{z} = \bar{z}$.

4. Иногда деление комплексных чисел можно выполнить быстрее, чем пользуясь непосредственным определением:

$$\frac{8 - 27i}{2 + 3i} = \frac{2^3 + 3^3 i}{2 + 3i} = 2^2 - 6i - 9 = -5 - 6i.$$

Далее *множество всех комплексных чисел* обозначается $\mathbb{C}$.

Упражнение 86. Проверьте, что для любых $z, w \in \mathbb{C}$

$$\overline{z \pm w} = \bar{z} \pm \bar{w}, \quad \overline{zw} = \bar{z} \cdot \bar{w}, \quad \overline{z/w} = \bar{z}/\bar{w},$$

где в последнем тождестве, естественно, $w \neq 0$.

На алгебраическом жаргоне предыдущее утверждение сформулировали бы так: *операция сопряжения является автоморфизмом поля $\mathbb{C}$.*

Это утверждение обобщается в следующей теореме.

Теорема 93. Пусть $f(z)$ — произвольный многочлен с комплексными коэффициентами, а многочлен $f^*(z)$ получается из него заменой всех коэффициентов на сопряженные. Тогда $f^*(\bar{z}) = \overline{f(z)}$ и, в частности, если все коэффициенты $f(z)$ действительные, то $f(\bar{z}) = \overline{f(z)}$.

Доказательство. Пусть $f(z) = a_n z^n + \dots + a_0$, тогда, применяя индукцию и тождества упражнения 86, имеем

$$\overline{a_n z^n + \dots + a_0} = \overline{a_n z^n} + \dots + \overline{a_0} = \overline{a_n} \overline{z^n} + \dots + \overline{a_0} = \overline{a_n} (\bar{z})^n + \dots + \overline{a_0} = f^*(\bar{z}). \quad \square$$

Следствие из теоремы 93. Пусть $f(z)$ — произвольный многочлен с комплексными коэффициентами, а многочлен $f^*(z)$ получается из него заменой всех коэффициентов на сопряженные. Тогда

$$f^*(z) = 0 \quad \Leftrightarrow \quad f(\bar{z}) = 0$$

и, в частности, если все коэффициенты $f(z)$ действительные, то

$$f(z) = 0 \quad \Leftrightarrow \quad f(\bar{z}) = 0.$$

Определение 96. Скалярным произведением чисел $z = a + ib$ и $w = c + id$ назовем число $\langle w, z \rangle = \operatorname{Re}(w\bar{z}) = ac + bd$.

Упражнение 87. Проверьте следующие свойства скалярного произведения:

- а) симметричность: $\langle w, z \rangle = \langle z, w \rangle$;
- б) однородность: $a\langle w, z \rangle = \langle aw, z \rangle$ для любого $a \in \mathbb{R}$;
- в) аддитивность $\langle w_1 + w_2, z \rangle = \langle w_1, z \rangle + \langle w_2, z \rangle$;
- г) неотрицательность квадрата (положительная определенность) $\langle z, z \rangle = |z|^2 \geq 0$.

Определение 97. Числа z и w назовем ортогональными, если $\langle w, z \rangle = 0$.

Упражнение 88. Проверьте, что

- а) числа z и iz всегда ортогональны,
- б) числа z и w ортогональны $\Leftrightarrow z = iaw$, где $a \in \mathbb{R}$.

Упражнение 89. Выведите из упражнения 86, что модули комплексных чисел удовлетворяют следующим тождествам: $|zw| = |z| \cdot |w|$,

$$\left| \frac{z}{w} \right| = \frac{|z|}{|w|}.$$

Упражнение 90. а) Запишите первое из двух предыдущих тождеств, заменяя модули их выражениями через действительные и мнимые части. Полученное тождество называется *тождеством Фибоначчи* и было открыто задолго до появления комплексных чисел.

б) Докажите его непосредственно.

в) Натуральное число назовем *шумерским*, если оно является суммой двух квадратов натуральных чисел. Докажите, что произведение шумерских чисел — шумерское число.

г) Проверьте тождество $\langle w, z \rangle^2 + \langle iw, z \rangle^2 = |z|^2 |w|^2$. У к а з а н и е. Так как $\operatorname{Re}(iz) = -\operatorname{Im} z$, то $\langle iw, z \rangle = \operatorname{Re}(iw\bar{z}) = -\operatorname{Im}(w\bar{z})$, значит,

$$\langle w, z \rangle^2 + \langle iw, z \rangle^2 = \operatorname{Re}(w\bar{z})^2 + \operatorname{Im}(w\bar{z})^2 = |w\bar{z}|^2 = |z|^2 |w|^2.$$

д) Проверьте, что предыдущее тождество — это просто другая запись тождества Фибоначчи.

Из тождества Фибоначчи немедленно следует частный случай неравенства Коши—Буняковского—Шварца $|\langle w, z \rangle| \leq |z| \cdot |w|$.

Упражнение 91. Проверьте, что в равенство оно обращается тогда и только тогда, когда $z = aw$, где $a \in \mathbb{R}$.

Из неравенства $|\langle w, z \rangle| \leq |z| \cdot |w|$ немедленно следует неравенство треугольника $|z| + |w| \geq |z + w|$. Действительно, согласно упражнению 87 и неравенству Коши—Буняковского

$$\begin{aligned} |z + w|^2 &= \langle w + z, w + z \rangle = \langle w, w \rangle + \langle z, z \rangle + 2\langle w, z \rangle \leq \\ &\leq |w|^2 + |z|^2 + 2|z||w| = (|z| + |w|)^2. \end{aligned}$$

Для комплексных чисел есть удобная геометрическая интерпретация * — их изображают точками плоскости с координатами (a, b) .

Эквивалентным образом, их можно изображать векторами, выходящими из начала координат и с концом в точке (a, b) (рис. 24). Множество всех действительных чисел при этом изображается одной из осей координат, называемой *действительной осью*, а множество всех чисто мнимых чисел, т. е. чисел с нулевой действительной частью, изображается другой осью координат, называемой *мнимой осью*. Модулем комплексного числа является длина изображающего его вектора.

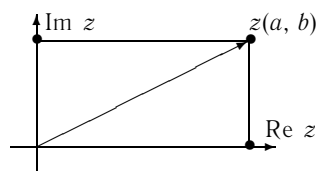


Рис. 24

* Предложенная в начале XIX в. независимо французом Ж. Арганом и датчанином К. Весселем, но вошедшая во всеобщее употребление благодаря Гауссу.

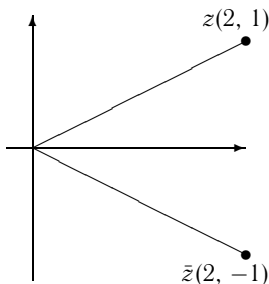


Рис. 25. Операция
сопряжения
 $0 \leq \arg z < 2\pi$.

Очевидно, например, что на комплексной плоскости числа z и $\bar{z}$ расположены симметрично относительно действительной оси (рис. 25).

Операция сложения комплексных чисел интерпретируется как сложение векторов (рис. 26).

Определение 98. Угол φ , образованный вектором z и положительным направлением действительной оси Ox , называется *аргументом* комплексного числа z и обозначается $\arg z$.

Аргумент определяется только для ненулевых чисел и обычно берется в пределах

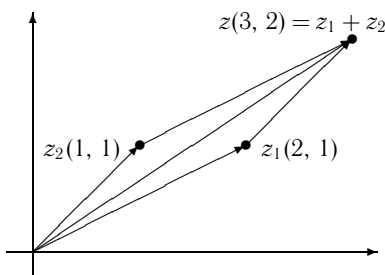


Рис. 26. Сложение комплексных чисел

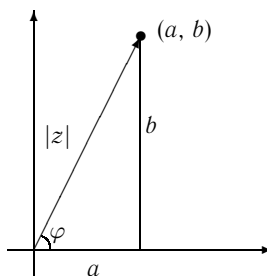


Рис. 27. Тригонометрическая форма

Примеры. 1. $\arg(1 + i) = \pi/4$. 2. $\arg(1 - i) = 7\pi/4$. 3. $\arg(-1 - i) = 5\pi/4$. 4. $\arg(-1 + i) = 3\pi/4$.

Из треугольника, изображенного на рис. 27, легко выразить тригонометрические функции от аргумента φ :

$$\cos \varphi = \frac{a}{\sqrt{a^2 + b^2}}, \quad \sin \varphi = \frac{b}{\sqrt{a^2 + b^2}}, \quad \operatorname{tg} \varphi = \frac{b}{a}.$$

Отсюда

$$a = \sqrt{a^2 + b^2} \cos \varphi = |z| \cos \varphi,$$

$$b = \sqrt{a^2 + b^2} \sin \varphi = |z| \sin \varphi,$$

значит,

$$z = a + bi = |z|(\cos \varphi + i \sin \varphi).$$

Получившаяся (так называемая тригонометрическая) форма записи числа z удобна при умножении.

Упражнение 92. Используя тригонометрические теоремы сложения, проверьте, что если

$$z_1 = |z_1|(\cos \varphi_1 + i \sin \varphi_1), \quad z_2 = |z_2|(\cos \varphi_2 + i \sin \varphi_2),$$

то

$$z_1 \cdot z_2 = |z_1 \cdot z_2|(\cos(\varphi_1 + \varphi_2) + i \sin(\varphi_1 + \varphi_2)),$$

$$\frac{z_1}{z_2} = \frac{|z_1|}{|z_2|}(\cos(\varphi_1 - \varphi_2) + i \sin(\varphi_1 - \varphi_2)).$$

В последнем равенстве предполагается, конечно, что $z_2 \neq 0$.

Упражнение 93. Из предыдущих равенств выведите, что

$$\arg(z_1 z_2) = (\arg z_1 + \arg z_2) \bmod 2\pi, \quad \arg \frac{z_1}{z_2} = (\arg z_1 - \arg z_2) \bmod 2\pi.$$

Применяя индукцию, докажите, что

$$\arg(z_1 z_2 \dots z_n) = (\arg z_1 + \arg z_2 + \dots + \arg z_n) \bmod 2\pi.$$

Упражнение 94. Докажите, что при умножении чисел z_i всегда на диаграмме Весселя—Аргана (рис. 28) треугольники с вершинами в точках $(0, 0)$, $(1, 0)$, z_1 и $(0, 0)$, z_2 , z подобны.

Упражнение 95. Постройте циркулем и линейкой сумму, разность, произведение и частное двух данных комплексных чисел (единица масштаба, действительная и мнимая оси заданы). Попробуйте сделать это самым экономным образом.

Скалярное произведение чисел z и w теперь, оказывается, совпадает со скалярным произведением векторов z и w , которое геометрически определяется как произведение длин векторов на косинус угла между ними.

Упражнение 96. Проверьте, что действительно для ненулевых векторов

$$|z||w| \cos \arg(w/z) = \operatorname{Re}(w\bar{z}) = \langle w, z \rangle.$$

Теперь мы можем использовать комплексные числа для доказательства геометрических теорем. Например, теорему о высотах треугольника можно доказать следующим образом. Пусть дан треугольник ABC (см. рис. 29). Выберем систему координат так, чтобы основание AB

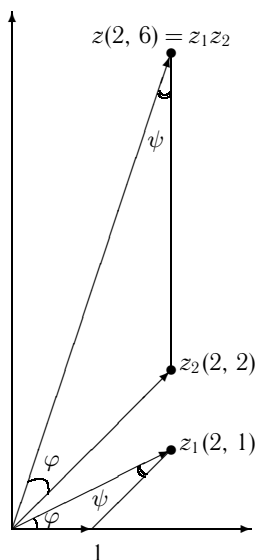


Рис. 28. Умножение комплексных чисел

лежало на действительной оси, а мнимая ось проходила по высоте CO , где O совпадает с началом координат. Тогда вершины треугольника A, B изображаются действительными числами a, b , а вершина C — чисто мнимым числом ic . Тогда ортоцентру H (точке пересечения высот) треугольника ABC отвечает чисто мнимое число $\frac{-iab}{c}$. Действительно, вектор AH соответствует числу $a + (iab)/c$, а вектор BC — числу $b - ic$, а согласно упражнению 88 эти вектора ортогональны (перпендикулярны), так как $a + (iab)/c = (b - ic)ia/c$, аналогично BH ортогонален AC , так как $b + (iab)/c = (a - ic)ib/c$, а ортогональность OH и AB ясна из условия.

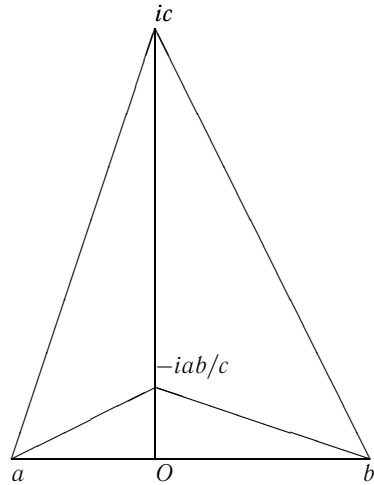


Рис. 29. Теорема об ортоцентре

Неравенства $|z_1| - |z_2| \leq |z_1 \pm z_2| \leq |z_1| + |z_2|$ можно интерпретировать на комплексной плоскости как неравенства треугольника. Первое из них уже было доказано. Второе неравенство следует из первого при смене знака у z_2 .

Упражнение 97. а) Найдите условие обращения неравенства треугольника в равенство с помощью комплексных чисел.

б) Докажите неравенство $|z_1 + z_2| \leq |z_1| + |z_2|$ с использованием действительных чисел, сведя его к неравенству $\sqrt{x_1^2 + y_1^2} + \sqrt{x_2^2 + y_2^2} \geq \sqrt{(x_1 + x_2)^2 + (y_1 + y_2)^2}$.

в) Докажите неравенство $|z_1 \pm \dots \pm z_n| \leq |z_1| + \dots + |z_n|$.

С помощью тригонометрической формы доказывается следующая теорема.

Теорема 94 (формула Муавра). Если $z = r(\cos \alpha + i \sin \alpha)$, то при любом натуральном n

$$z^n = r^n(\cos n\alpha + i \sin n\alpha).$$

Доказательство. Доказательство проводится по индукции. База индукции ($n = 1$) очевидна. Шаг индукции обосновывается с помощью упражнения 92. Легко видеть, что формула Муавра верна и для отрицательных целых n . $\square$

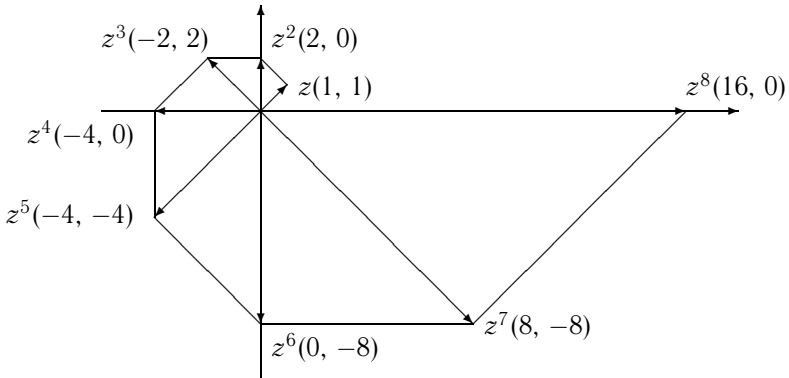


Рис. 30. Возведение в степень комплексных чисел

На рис. 30 видно, что точки w^n укладываются на спиральную линию, состоящую из точек w , удовлетворяющих условию

$$|w| = e^{\arg w}.$$

Упражнение 98. Найдите эту константу c , соответствующую изображенным числам.

Свойство этой спирали не изменяться при преобразованиях подобия так потрясло Якоба Бернулли *, что согласно завещанию ее изображали на его могильной плите в Базельском соборе с надписью «Eadem mutata resurgo» **. Кроме Бернулли, ее изучали ранее Декарт и Торичелли. Любопытно, что логарифмическая спираль используется в технике и даже встречается в живой природе (ее можно увидеть на раковине моллюска *Haliotis splendis*, а также внимательно разглядывая расположение семечек в подсолнухе).

Задачи и упражнения к § 4.3

1. Вычислите $(29 + 23i)/(1 + 5i)$.
2. Докажите, что:
 - а) точки $1 + 4i$, $2 + 7i$, $3 + 10i$ лежат на одной прямой;
 - б) точки $2 + i$, $4 + 4i$, $6 + 9i$, $8 + 16i$ лежат на одной параболе.

* Я. Бернулли (Jacob Bernoulli, 1654–1705) — знаменитый швейцарский математик. Брат не менее знаменитого Иоганна Бернулли.

** Измененная, воскресаю прежней (*лат.*).

3. Докажите неравенство треугольника с помощью тригонометрической формы.

У к а з а н и е. Пусть $z_1 = r_1(\cos \varphi_1 + i \sin \varphi_1)$, $z_2 = r_2(\cos \varphi_2 + i \sin \varphi_2)$, тогда $z_1 + z_2 = r_1 \cos \varphi_1 + r_2 \cos \varphi_2 + i(r_1 \sin \varphi_1 + r_2 \sin \varphi_2)$, откуда

$$\begin{aligned} |z_1 + z_2|^2 &= (r_1 \cos \varphi_1 + r_2 \cos \varphi_2)^2 + (r_1 \sin \varphi_1 + r_2 \sin \varphi_2)^2 = \\ &= r_1^2 + 2r_1 r_2 \cos(\varphi_1 - \varphi_2) + r_2^2 \leq (r_1 + r_2)^2 = (|z_1| + |z_2|)^2. \end{aligned}$$

4. Какие части комплексной плоскости $\mathbb{C}$ выделяются условиями: $\operatorname{Re} z > 0$, $\operatorname{Re} z \geq 0$, $\operatorname{Re} z = 0$, $a \leq \operatorname{Im} z \leq b$, $|z - z_0| = R$, $|z - z_0| < R$, $R \leq |z| \leq R'$, $\operatorname{Re} 1/z = 1/R$?

5. Найдите множество точек на комплексной плоскости $\mathbb{C}$, удовлетворяющее условиям:

- а) $|z - a| + |z - b| = k$ (эллипс);
- б) $|z - a| + |z - b| \leq k$;
- в) $|z - a| - |z - b| = k$ (гипербола);
- г) $|z - a|/|z - b| = k$ (окружность Аполлония);
- д) $|z - a|/|1 - \bar{a}z| < 1$;
- е) $|z - a|/|1 - \bar{a}z| > 1$.

6. Отображение комплексной плоскости $\mathbb{C}$ в себя, задаваемое формулой $w = iz$, есть поворот вокруг начала координат на угол 90° .

7. Отображение комплексной плоскости $\mathbb{C}$ в себя, задаваемое формулой $w = az$, $|a| = 1$, есть поворот вокруг начала координат.

8. Отображение комплексной плоскости $\mathbb{C}$ в себя, задаваемое формулой $w = az + b$, $a, b \in \mathbb{C}$, есть подобие первого рода (не меняющее ориентации), при $|a| = 1$ — движение (т. е. преобразование, не меняющее расстояния между точками), при $a = 1$ — параллельный перенос.

9*. Отображение комплексной плоскости в себя, задаваемое формулой $w = 1/\bar{z}$, есть инверсия с центром в 0 относительно окружности $|z| = 1$.

10. Найдите максимум и минимум $|z|$ при условии

$$\left| z + \frac{1}{z} \right| = a.$$

11. Отображение $\mathbb{C}$ в $\mathbb{C}$, задаваемое формулой

$$w = \frac{az + b}{cz + d}, \quad a, b, c, d \in \mathbb{C}, \quad ad - bc \neq 0,$$

переводит прямую и окружность в прямую или окружность и сохраняет углы между ними.

12. Если точки z_k лежат на одной прямой, то $(z_1 - z_2)/(z_2 - z_3) \in \mathbb{R}$, и обратно.

13. Если точки z_k лежат на одной окружности, то

$$((z_1 - z_3)/(z_2 - z_3))/((z_1 - z_4)/(z_2 - z_4)) \in \mathbb{R},$$

и обратно.

14*. Найдите наибольшее натуральное n такое, что существуют числа $z_1, \dots, z_n \in \mathbb{C}$, для которых $\min_{i \neq j} |z_i - z_j| \geq \max_i |z_i|$. Найдите эти числа.

15. Если стороны треугольника удовлетворяют равенству

$$a^2 + b^2 + c^2 = ab + bc + ac,$$

то треугольник правильный.

16. Если вершинами треугольника на комплексной плоскости являются числа u, v, w , удовлетворяющие равенству

$$u^2 + v^2 + w^2 = uv + vw + uw,$$

то треугольник правильный.

17. Если вершинами треугольника на комплексной плоскости являются числа u, v, w , то его центр тяжести (точка пересечения медиан) изображается числом $(u + v + w)/3$.

18. Докажите неравенство Птолемея: для любого четырехугольника $ABCD$

$$|AD||BC| \leq |BD||AC| + |CD||AB|.$$

У к а з а н и е. Примените тождество для комплексных чисел

$$(a - d)(c - b) + (b - d)(a - c) + (c - d)(b - a) = 0$$

и выведите из него с помощью неравенства треугольника, что

$$|a - d||b - c| \leq |b - d||a - c| + |c - d||a - b|.$$

19. Докажите, что для четырехугольника $ABCD$ равенство

$$|AD||BC| = |BD||AC| + |CD||AB|$$

справедливо тогда и только тогда, когда вокруг него можно описать окружность.

У к а з а н и е. Примените указание к задаче 18 и задачу 13.

20. Докажите тождества и предложите для них геометрическую интерпретацию:

а) $|z + w|^2 + |z - w|^2 = 2(|z|^2 + |w|^2),$

б) $|z| + |w| = |(z + w)/2 - \sqrt{zw}| + |(z + w)/2 + \sqrt{zw}|.$

У к а з а н и е. $\sqrt{a} = b$, если $b^2 = a$.

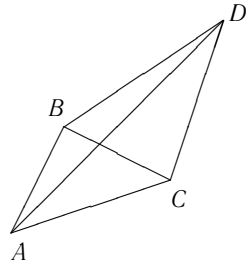


Рис. 31. Теорема Птолемея

21. Докажите, что отображение $w = (1 + iz)/(1 - iz)$ переводит полуплоскость $\text{Im } z \geq 0$ в круг $|w| \leq 1$.

22. Пусть $|z| = |u| = |w|$. Докажите, что

$$\left| \frac{zu + uw + zw}{z + u + w} \right| = |z|.$$

Докажите, что при условии $|z| = |u| = |w|$ следующие утверждения эквивалентны:

а) точки z, u, w образуют правильный треугольник, т. е. $|z - w| = |z - u| = |u - w|$,

б) справедливо равенство $z + u + w = 0$,

в) числа z, u, w являются корнями уравнения вида $x^3 = v, v \in \mathbb{C}$.

23. Пусть $|z_1| = |z_2| = |z_3| = |z_4|$. Докажите, что следующие утверждения эквивалентны:

а) точки z_i образуют прямоугольник,

б) справедливо равенство $z_1 + z_2 + z_3 + z_4 = 0$,

в) числа z_i являются корнями уравнения вида

$$(z^2 - a^2)(z^2 - b^2) = 0, \quad |a| = |b| \neq 0.$$

24. Пусть $|z| = 1$. Докажите, что $\left| \frac{z-1}{\bar{a}} \right| = \frac{|z-a|}{|a|}$.

25*. Решите в действительных и комплексных числах системы

$$\begin{cases} x - \frac{x-3y}{x^2+y^2} = 2; \\ y + \frac{3x+y}{x^2+y^2} = 3; \end{cases} \quad \begin{cases} x^2 - y^2 - \frac{x+3y}{x^2+y^2} = 2; \\ 2xy + \frac{3x+y}{x^2+y^2} = 3. \end{cases}$$

26. Можно в качестве основания позиционной системы счисления выбирать даже комплексные числа, например, при выборе основания $b = 2i$ получается «мнимочетверичная» система. В качестве цифр в ней используются 0, 1, 2, 3, и запись $(a_n, \dots, a_0, a_{-1}, \dots, a_{-k})_{2i}$ означает

$$\sum_{s=-k}^n a_s \cdot (2i)^s.$$

Проверьте, что

$$\begin{aligned} (a_{2n} \dots a_0, a_{-1} \dots a_{-2k})_{2i} = \\ = (a_{2n} \dots a_2, a_{-2} \dots a_{-2k})_{-4} + 2i(a_{2n-1} \dots a_1, a_{-1} \dots a_{-2k+1})_{-4}. \end{aligned}$$

В этой системе любое комплексное число с двоично-рациональными компонентами можно записать без знака и без деления на действительную и мнимую часть.

27. Модифицируйте алгоритм умножения столбиком, чтобы он позволял умножать числа и в мнимочетверичной системе.

Заметьте, что этот алгоритм умножает комплексные числа без разделения действительных и мнимых частей.

28*. Дано, что $\sum_{i=1}^n z_i = 0$. Докажите, что существуют i, j такие, что

$$|\arg z_i - \arg z_j| \geq \frac{2\pi}{3}.$$

29*. Если точку $a \in \mathbb{C}$ можно отделить некоторой прямой от точек $z_1, \dots, z_n \in \mathbb{C}$, то $\sum_{i=1}^n 1/(z_i - a) \neq 0$.

30*. (Гаусс—Люка.) Докажите, что корни производной многочлена лежат внутри наименьшего выпуклого многоугольника, содержащего все корни этого многочлена.

31. Примените формулу Муавра для вывода тригонометрических формул двойного и тройного угла.

32. Примените формулу Муавра для выражения $\sin nx$ и $\cos nx$ в виде многочленов от $\sin x, \cos x$.

33*. Вычислите $\sum_{k=0}^n q^k \cos(kx + \alpha)$.

34*. Вычислите $\sum_{k=0}^n \cos^2 kx$.

35*. Вычислите $\sum_k C_n^{3k+r}, r = 0, 1, 2$.

36*. Докажите, что

$$\sum_k (-1)^k C_n^{2k} = 2^{n/2} \cos n\pi/4, \quad \sum_k (-1)^k C_n^{2k+1} = 2^{n/2} \sin n\pi/4.$$

37*. Докажите неравенство $\sum_{k,i=1}^n \cos(x_k - x_i) \geq 0$.

§ 4.4. Вычисления на калькуляторе

Даже на многих хороших калькуляторах отсутствует прямая возможность вычислений с комплексными числами. Тем не менее покажем на примере отечественного калькулятора МК-71 несколько удобных способов работы с комплексными числами.

Начнем со сложения-вычитания нескольких чисел. Эта операция сводится к сложению-вычитанию двух чисел $(a + ib) \pm (c + id)$. Действительные и мнимые части этих чисел придется вводить в калькулятор

по отдельности. Для того чтобы полученный результат можно было не переписывать на бумагу и заново вводить в калькулятор, нужно сохранить действительную часть результата $a + c$ на индикаторе, а мнимую часть запомнить в памяти.

Ячейку памяти и ее содержимое обозначаем далее Π , запись числа с индикатора в память обозначаем, как и на кнопке калькулятора, $x \rightarrow \Pi$, вызов числа из памяти на индикатор обозначаем $\Pi \rightarrow x$, обмен содержимым между памятью и калькулятором выполняется кнопкой $\leftrightarrow$, но только после предварительного нажатия на специальную кнопку F , ввод числа a на индикатор обозначаем просто a .

Сложение-вычитание $(a + ib) \pm (c + id)$ можно с выполнением указанного условия выполнить следующей последовательностью операций (в записи они задаются названиями соответствующих кнопок и разделяются для удобства запятыми):

$$a, \pm, c, x \rightarrow \Pi, b, \pm, d, F, \leftrightarrow.$$

Если после выполнения этой операции мы хотим к результату прибавить еще число $e + fi$, то, так как после обмена $\leftrightarrow$ на индикаторе опять возникла действительная часть результата, достаточно выполнить следующую последовательность операций

$$+, e, F, \leftrightarrow, +, f, F, \leftrightarrow$$

и далее ее повторять, пока выполняем сложения-вычитания.

Заметим, что в этом способе нам приходится каждое из заданных чисел вводить только один раз, а промежуточные результаты запоминает сам калькулятор.

Однако умножить два числа $(a + ib)(c + id)$ без записи и повторного ввода промежуточных результатов так просто не удастся. Можно, конечно, сделать это так:

$$a, \cdot, c, -b, \cdot, d, b, \cdot, c, +, a, \cdot, d,$$

пользуясь тем, что при вычислении выражений типа скалярных произведений $ac - bd$ промежуточные результаты запоминать не нужно, но если мы запомним действительную часть результата $ac - bd$, то числа d, b, c , a придется вводить второй раз.

Еще хуже дело обстоит с делением. Так как

$$z = \frac{a + ib}{c + id} = \frac{ac + bd}{c^2 + d^2} + \frac{bc - ad}{c^2 + d^2}i,$$

непосредственное использование этой формулы требует 11 арифметических операций.

Если вычислять по схеме

$$r = d/c, \quad s = c + dr, \quad \operatorname{Re} z = (a - br)/s, \quad \operatorname{Im} z = (b - ar)/s,$$

то достаточно 9 операций. Но и здесь числа a , b , r придется вводить по два раза.

Можно доказать, что меньшим числом операций обойтись нельзя.

Но если сомножители заданы в тригонометрической форме, то аналогично сложению-вычитанию можно вычислить любую комплексную дробь вида $z = z_1 \circ \dots \circ z_n$, где знак « $\circ$ » обозначает умножение или деление без лишних операций ввода чисел.

Как же на калькуляторе преобразовать комплексное число в тригонометрическую форму? Это можно сделать с помощью кнопки $R \rightarrow P$, которая предназначена для перевода декартовых координат в полярные. После последовательности операций

$$\operatorname{Re} z, F, P \rightarrow R, \operatorname{Im} z, =$$

на индикаторе появляется $|z|$, если потом нажать кнопки $F, \leftrightarrow$ (или $x \rightarrow \Pi$), то $|z|$ окажется в памяти, но если после этого нажать кнопку $\leftrightarrow$ без предварительного нажатия кнопки F , то на индикаторе появится полярный угол, а число в памяти не изменится. Можно и не запоминать предварительно $|z|$, а сразу нажать кнопку $\leftrightarrow$, тогда на индикаторе тоже появится полярный угол, но $|z|$ безвозвратно пропадет.

Полярный угол совпадает с аргументом, если $\operatorname{Im} z \leq 0$, и равен $\arg z - 2\pi$, если $\operatorname{Im} z < 0$, но так как по модулю 2π они совпадают, то полярный угол можно использовать при умножении-делении чисел вместо аргумента с тем же успехом.

Для обратного перехода от полярных координат к декартовым нужно выполнить последовательность операций

$$|z|, F, R \rightarrow P, \varphi, =,$$

после чего на индикаторе появится $\operatorname{Re} z$, а если нажать кнопку $\leftrightarrow$, то на индикаторе появится $\operatorname{Im} z$. Для того чтобы не пропало число $\operatorname{Re} z$, его предварительно можно занести в память. Если одно из чисел $|z|$, φ находится в памяти, его оттуда надо предварительно извлечь, нажав кнопку $\Pi \rightarrow x$. Заметим, что если вместо полярного угла ввести любое равное ему по модулю 2π число, то результат не меняется.

Если числа в дроби вида $z_1 \circ \dots \circ z_n$ заданы не в полярных, а в декартовых координатах, то неудобно их предварительно переводить в полярные координаты перед вычислением дроби. Можно вычислить по отдельности модуль и аргумент произведения, а потом преобразовать результат к стандартному виду.

Вначале можно вычислить (по модулю 2π) $\arg z$ с помощью последовательности операций

$$\text{Re } z_1, F, R \rightarrow P, \text{Im } z_1, =, \leftrightarrow, (-,)\Pi+, \text{Re } z_2, F, R \rightarrow P, \text{Im } z_2, =, \leftrightarrow, (-,)\Pi+, \dots, \text{Re } z_1, F, R \rightarrow P, \text{Im } z_1, =, \circ, \text{Re } z_2, F, R \rightarrow P, \text{Im } z_2, =, \circ, \dots,$$

при этом вначале надо обнулить память. После каждой операции $F, R \rightarrow P$ нажимаем кнопку $\leftrightarrow$, чтобы вызвать на индикатор вычисленный $\arg z_i$, потом, если надо, меняем у него знак кнопкой « $-$ » и прибавляем к числу в памяти кнопкой $\Pi+$.

Потом вычисляем $|z|$ последовательностью операций

$$\text{Re } z_1, F, R \rightarrow P, \text{Im } z_1, =, \circ, \text{Re } z_2, F, R \rightarrow P, \text{Im } z_2, =, \circ, \dots$$

Для возведения в n -ю степень числа z есть более быстрый алгоритм. Для этого выполняем следующую последовательность операций:

$$\begin{aligned} \text{Re } z, F, R \rightarrow P, \text{Im } z, =, F, \leftrightarrow, \leftrightarrow, \cdot, n, =, F, \leftrightarrow, F, y^x, n, =, F, P \rightarrow R, \\ \Pi \rightarrow x, \leftrightarrow, x \rightarrow \Pi, \leftrightarrow, \end{aligned}$$

при этом на индикаторе появится $\text{Re } z^n$, а в памяти окажется $\text{Im } z^n$.

Рассмотрим теперь вопрос о решении кубических уравнений с действительными коэффициентами на калькуляторе.

Начать естественно с преобразования уравнения $x^3 + ax^2 + bx + c = 0$ к виду $x^3 + px + q = 0$. Делается это заменой $x' = x + a/3$, тогда

$$p = b - a^2/3, \quad q = 2a^3/27 - ab/3 + c.$$

Удобный алгоритм для вычисления p, q на калькуляторе таков:

$$a, a \rightarrow \Pi, \cdot, /, -3, +, b, F, \leftrightarrow, \cdot, /, 9, \Pi+, \sqrt{\cdot}, -, \cdot, \Pi \rightarrow x, +, c.$$

Число q оказывается на индикаторе, а p остается в памяти.

Использовать формулу Кардано—Тартальи для вычислений неудобно, так как придется неоднократно записывать промежуточные результаты. Поэтому преобразуем уравнение $x^3 + px + q = 0$ к виду $4x^3 \pm 3x + r = 0$ заменой $x = 2\sqrt{|p|/3}x'$, тогда $r = \sqrt{27}q/(2|p|^{3/2})$.

Рассмотрим три возможных случая.

1. Пусть $4x^3 - 3x + r = 0$, $|r| \leq 1$. Это рассмотренный нами ранее неприводимый случай, и тогда корни находятся по формулам (ранее мы использовали косинусы, но с тем же успехом годятся и синусы)

$$x_1 = \sin \varphi, \quad x_{2,3} = \sin(\varphi \pm 2\pi/3),$$

где $r = \sin 3\varphi$.

На калькуляторе эти корни вычисляются следующим образом:

$$r, F, \sin, /, 3, x \rightarrow \Pi, \sin(=x_1), \pi, \cdot, 2, /, 3, +, \\ \Pi \rightarrow x, \sin(=x_2), \pi, \cdot, -2, /, 3, +, \Pi \rightarrow x, \sin(=x_3).$$

2. Пусть $4x^3 - 3x + r = 0$, $|r| > 1$.

Определение 99. Назовем *гиперболическим косинусом* функцию

$$\operatorname{ch} \varphi = \frac{e^\varphi + e^{-\varphi}}{2},$$

а *гиперболическим синусом* — функцию

$$\operatorname{sh} \varphi = \frac{e^\varphi - e^{-\varphi}}{2}.$$

Калькулятор вычисляет функцию $\operatorname{sh} \varphi$, если нажать кнопку hyp , а потом кнопку $\sin$. Для краткости будем обозначать эту комбинацию кнопок как sinh , аналогично будем писать cosh для гиперболического косинуса.

Упражнение 99.

- а) Функция $\operatorname{sh} \varphi$ нечетная и строго монотонно возрастающая.
- б) Функция $\operatorname{ch} \varphi$ четная.

Поэтому функция $\operatorname{sh} \varphi$ имеет обратную функцию, которую калькулятор вычисляет, если нажать кнопки F , потом hyp , а потом кнопку $\sin$.

Можно считать, что функция $\operatorname{ch} \varphi$ тоже имеет обратную, и в качестве ее значения выбирается *положительное* значение φ , для которого $\operatorname{ch} \varphi = x$. В отличие от обратного гиперболического синуса, обратный косинус определен только при $x \geq 1$. Вычисляется он на калькуляторе аналогично обратному синусу.

Тогда, если $r = (\operatorname{sign} r) \operatorname{ch} 3\varphi$, где $\operatorname{sign} r = 1$ при $r > 0$ и $\operatorname{sign} r = -1$ при $r < 0$, то корни уравнения находятся по формулам

$$x_1 = -(\operatorname{sign} r) \operatorname{ch} \varphi, \quad x_{2,3} = \frac{1}{2}(\operatorname{sign} r)(\operatorname{ch} \varphi \pm i\sqrt{3} \operatorname{sh} \varphi).$$

Например, в случае $r > 0$ корни вычисляются следующим образом:

$$r, F, \cosh, /, 3, x \rightarrow \Pi, \cosh, -, (=x_1), \Pi \rightarrow x, \\ \cosh, /, 2, 3, \sqrt{, /, 2, \cdot, \Pi \rightarrow x, \sinh, -.$$

3. Пусть $4x^3 + 3x + r = 0$. Тогда, если $r = -\operatorname{sh} 3\varphi$, то корни уравнения находятся по формулам

$$x_1 = \operatorname{sh} \varphi, \quad x_{2,3} = -\frac{1}{2}(\operatorname{sh} \varphi \pm i\sqrt{3} \operatorname{ch} \varphi).$$

На калькуляторе они вычисляются следующим образом: $r, -, F, \sinh, /, 3, x \rightarrow \Pi, \sinh(=x_1), \Pi \rightarrow x, \sinh, /, -2, 3, \sqrt{, /, 2, \cdot, \Pi \rightarrow x, \cosh, -.$

Задачи и упражнения к § 4.4

1. Проверить и обосновать указанные в этом параграфе алгоритмы.
2. Выведите формулы для p, q через a, b, c в преобразовании уравнения $x^3 + ax^2 + bx + c = 0$ к виду $x^3 + px + q = 0$.
3. Докажите формулу $r = \sqrt{27}q/(2|p|^{3/2})$.
4. Покажите, как использовать в решении неприводимого случая косинус вместо синуса.
5. Докажите, что $\operatorname{ch}^2 \varphi - \operatorname{sh}^2 \varphi = 1$.
6. Выразите обратные гиперболические функции через логарифмы.
7. Выведите теоремы сложения для гиперболических синуса и косинуса.
8. Выведите формулы тройного угла для гиперболических синуса и косинуса.
- 9*. Выведите формулы для решения кубических уравнений в остальных двух случаях.
- 10*. Как перемножить два комплексных числа, используя только три действительных умножения?

§ 4.5. Корни из комплексных чисел

С помощью формулы Муавра можно извлекать корни из комплексных чисел. Пусть z — заданное комплексное число, отличное от 0, и ω — некоторый корень степени n из z , т. е. $\omega^n = z$. Положив

$$z = r(\cos \alpha + i \sin \alpha), \quad \omega = s(\cos \beta + i \sin \beta),$$

по формуле Муавра получим

$$s^n(\cos n\beta + i \sin n\beta) = r(\cos \alpha + i \sin \alpha).$$

Тем самым число z двумя способами представлено в тригонометрической форме, откуда

$$s = \sqrt[n]{r}, \quad \beta = \frac{\alpha + 2k\pi}{n}, \quad k \in \mathbb{Z}.$$

Таким образом, всякий корень степени n из числа z имеет вид:

$$\omega_k = \sqrt[n]{r} \left(\cos \frac{\alpha + 2k\pi}{n} + i \sin \frac{\alpha + 2k\pi}{n} \right), \quad k \in \mathbb{Z}.$$

Естественно, что для описания всех корней n -й степени из комплексного числа ω достаточно взять $k = 0, 1, \dots, n-1$.

Из формулы Муавра следует и обратное утверждение, что всякое число такого вида является корнем степени n из числа z , и, следовательно, эта формула описывает все множество корней из z .

Упражнение 100. Докажите, что для любого рационального числа p/q одно из значений $(r(\cos \alpha + i \sin \alpha))^{p/q}$ равно

$$r^{p/q} \left(\cos \frac{p}{q} \alpha + i \sin \frac{p}{q} \alpha \right)$$

(обобщенная формула Муавра).

Рассмотрим уравнение $z^n = 1$. По выше доказанному каждый из n корней этого уравнения имеет вид

$$\varepsilon_k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}, \quad (1)$$

где $k = 0, 1, \dots, n-1$.

На комплексной плоскости корни n -й степени из 1 располагаются в вершинах правильного n -угольника с центром в точке $(0, 0)$ и вершиной, соответствующей ε_0 , в точке $(1, 0)$.

Теорема 95. Множество корней n -й степени из единицы — циклическая группа порядка n относительно умножения.

Доказательство. Доказать, что множество корней n -й степени из 1 образует группу, можно непосредственной проверкой с использованием формулы (1). Другой способ доказательства использует тот факт, что корни n -й степени из единицы удовлетворяют условию $z^n = 1$, а значит, их произведение, обратный элемент и единица тоже удовлетворяют этому условию.

Для того чтобы доказать цикличность группы, достаточно указать образующий элемент. Очевидно, что по крайней мере одним из образующих будет $\varepsilon_1 = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$. Действительно, для любого $k = 0, 1, \dots, n-1$

$$\varepsilon_k = \varepsilon_1^k. \quad \square$$

Найдем все образующие этой группы.

Теорема 96. Число ε_m является образующей циклической группы корней n -й степени из единицы тогда и только тогда, когда числа n и m взаимно просты.

Доказательство. Доказательство может быть основано на линейном представлении НОД чисел n и m : $(n, m) = an + bm$, где $a, b \in \mathbb{Z}$. Но можно просто сослаться на теорему 31. $\square$

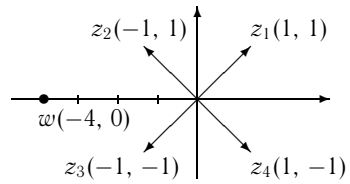


Рис. 32. Извлечение корней четвертой степени из числа w

Теорема 97. Все корни уравнения

$$\omega^n = z, \quad z \neq 0, \quad (2)$$

могут быть получены по формуле $\omega_i = \varepsilon_k \cdot \omega_m$, где ε_k — корень уравнения $\varepsilon^n = 1$, $k = 0, 1, \dots, n-1$, ω_m — один из корней уравнения (2).

Доказательство. Так как

$$\omega_m = |\omega| \left(\cos \frac{\alpha + 2m\pi}{n} + i \sin \frac{\alpha + 2m\pi}{n} \right), \quad m = 0, 1, \dots, n-1,$$

то

$$\begin{aligned} \omega_m \cdot \varepsilon_k &= |\omega| \left(\cos \left(\frac{\alpha + 2m\pi}{n} + \frac{2k\pi}{n} \right) + i \sin \left(\frac{\alpha + 2m\pi}{n} + \frac{2k\pi}{n} \right) \right) = \\ &= |\omega| \cdot \left(\cos \frac{\alpha + 2\pi(m+k)}{n} + i \sin \frac{\alpha + 2\pi(m+k)}{n} \right), \end{aligned}$$

причем $m+k$ пробегает полную систему вычетов по модулю n (т.е. любую систему из n чисел, попарно не сравнимых по модулю n), если то же верно для k . $\square$

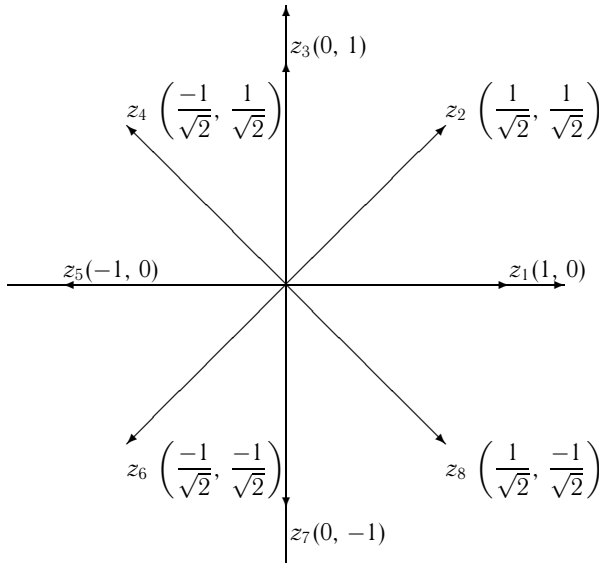


Рис. 33. Корни восьмой степени из единицы

Объясним теперь, что понимают под полярной и показательной формами записи комплексных чисел. Используя тригонометрическую форму

записи комплексных чисел, мы можем ввести для числа $z = r (\cos \varphi + i \sin \varphi)$ полярную форму записи (r, φ) . Полярная форма записи соответствует полярной системе координат, когда задано начало координат O , луч OB , а точка A , задаваемая комплексным числом (r, φ) , получается, если от этого луча отложить угол $\angle BOA = \varphi$, причем длина отрезка OA равна r , где $r > 0$. Число 0 в этой системе координат соответствует началу координат точке O .

В показательной форме записи комплексного числа z , т.е. в форме $e^{x+i\varphi} = e^x (\cos \varphi + i \sin \varphi)$, где $x = \ln(|z|) = \ln r$, формула умножения приобретет особенно красивый вид:

$$e^{x_1+i\varphi_1} \cdot e^{x_2+i\varphi_2} = e^{x_1+x_2} \cdot e^{(\varphi_1+\varphi_2)i} = e^{x_1+x_2+i(\varphi_1+\varphi_2)}.$$

Задачи и упражнения к § 4.5

1. Докажите, что

$$\sqrt{a+ib} = \pm \left(\sqrt{\frac{\sqrt{a^2+b^2}+a}{2}} + i \operatorname{sign} b \sqrt{\frac{\sqrt{a^2+b^2}-a}{2}} \right)$$

где $\operatorname{sign} b$ — знак числа $b \in \mathbb{R}$.

2. Постройте квадратные корни из данного числа с помощью циркуля и линейки наиболее экономным способом.

3. Постройте корни четвертой степени из данного числа с помощью циркуля и линейки наиболее экономным способом.

4. Изобразите извлечение корня шестой степени из единицы с помощью спичек.

5. Изобразите возведение во 2, 3, 4, 5-ю степень числа $3/2 + i\sqrt{3}/2$ с помощью спичек.

6. На плоскости даны два квадрата $A_i B_i C_i D_i$, $i = 1, 2$. Векторы OA , OB , OC , OD равны векторам $A_1 A_2$, $B_1 B_2$, $C_1 C_2$, $D_1 D_2$ соответственно. Докажите, что $ABCD$ — квадрат.

7. Найдите сумму всех корней n -й степени из единицы.

8. Найдите произведение всех корней n -й степени из единицы.

9. Найдите сумму k -х степеней всех корней n -й степени из единицы.

10. Докажите равенство

$$(a, b) = \sum_{m=0}^{a-1} \sum_{n=0}^{a-1} \frac{1}{a} e^{2\pi i b m n / a}.$$

11. Решите в действительных числах систему

$$\begin{cases} \sin x + \sin y + \sin z = 0; \\ \cos x + \cos y + \cos z = 0. \end{cases}$$

12. Решите в действительных числах систему

$$\begin{cases} \sin x + \sin y + \sin z = 1; \\ \cos x + \cos y + \cos z = 0. \end{cases}$$

13. Пусть $|z|, |u|, |w| \leq 1$. Докажите, что $|(z-u)(z-w)(u-w)|^2 \leq 27$.

14*. Правильный n -угольник вписан в единичную окружность. Докажите, что

- а) сумма квадратов всех его сторон и диагоналей равна n ;
- б) сумма всех его сторон и диагоналей равна $n \operatorname{ctg} \pi/2n$;
- в) произведение всех его сторон и диагоналей равно $n^{n/2}$.

15*. Обозначим вершины правильного n -угольника, вписанного в единичную окружность, через $A_1, \dots, A_n$ и продолжим нумерацию по кругу далее, так что $A_{n+1} = A_1$, $A_{n+2} = A_2$ и т. д. Докажите для нечетного n , что $|OA_1 + OA_4 + OA_9 + \dots + OA_{n^2}| = \sqrt{n}$, где O — центр n -угольника.

16*. Вершины правильного n -угольника раскрашены в несколько цветов так, что все одноцветные вершины образуют также правильные многоугольники. Докажите, что среди них найдутся хотя бы два одинаковых.

17*. Обозначим $f_n(x)$ многочлен со старшим коэффициентом 1, корнями которого являются первообразные корни n -й степени из 1 в поле $\mathbb{C}$ и только они. Этот многочлен называется n -м *круговым многочленом*. Докажите, что $f_n(x) \in \mathbb{Z}[x]$, $\deg f_n(x) = \varphi(n)$ и

$$x^n - 1 = \prod_{d|n} f_d(x).$$

18. Проверьте, что

$$\begin{aligned} f_1(x) &= x - 1, & f_2(x) &= x + 1, & f_3(x) &= x^2 + x + 1, \\ f_4(x) &= x^2 + 1, & f_5(x) &= x^4 + x^3 + x^2 + x + 1, & f_6(x) &= x^2 - x + 1, \\ f_7(x) &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, & f_8(x) &= x^4 + 1, \\ f_9(x) &= x^6 + x^3 + 1, & f_{10}(x) &= x^4 - x^3 + x^2 - x + 1. \end{aligned}$$

19. Разложите на множители: (i) $1 + x^6$; (ii) $1 + x^9$; (iii) $1 + x^5$; (iv) $1 + x^{15}$.

20*. Разложите на множители $1 + x^n$.

21*. (Мультипликативный вариант формулы обращения Мёбиуса.) Докажите, что если при любом n

$$g(n) = \prod_{d|n} f(d),$$

то

$$f(n) = \prod_{d|n} g(n/d)^{\mu(n)}.$$

22*. Докажите, что

$$f_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}.$$

23*. Докажите, что сумма первообразных корней n -й степени из 1 в поле $\mathbb{C}$ равна $\mu(n)$, а произведение их равно $(-1)^{\varphi(n)}$, и, значит,

$$f_n(x) = x^n - \mu(n)x^{n-1} + \dots + 1.$$

24*. Докажите, что при простом p

$$f_p(x) = x^{p-1} + x^{p-2} + \dots + 1,$$

и этот многочлен неприводим над полем рациональных чисел.

25*. Докажите, что при простом p и $k \geq 1$

$$f_{p^k}(x) = f_p(x^{p^{k-1}}) = x^{(p-1)p^{k-1}} + x^{(p-2)p^{k-1}} + \dots + 1,$$

и этот многочлен неприводим над полем рациональных чисел.

26*. Докажите, что $f_{2n}(x) = f_n(-x)$, если n нечетно.

27*. Докажите, что $f_{pn}(x) = f_n(x^p)/f_n(x)$, если p простое и n не кратно p .

28*. Докажите, что $f_{mn}(x) = f_n(x^m)$, если каждый простой делитель n делит также m .

29.** Докажите, что любой круговой многочлен неприводим над полем рациональных чисел.

30*. (Быстрый алгоритм вычисления кругового многочлена $f_n(x)$.) Находим все простые делители $p_1, \dots, p_m$ у числа n и вычисляем последовательно многочлены по формулам

$$g_0(x) = x - 1, \quad g_i(x) = g_{i-1}(x^{p_i})/g_{i-1}(x), \quad i = 1, \dots, m, \\ f_n(x) = g_m(x^{n/(p_1 \dots p_m)}).$$

Обоснуйте этот алгоритм.

31. Постройте из отрезков длины 1, 2, ..., 6 выпуклый равноугольный шестиугольник.

32*. Докажите, что из отрезков длины $1, 2, \dots, n$ нельзя составить выпуклый равноугольный n -угольник при n , равном степени простого, и можно его построить во всех остальных случаях.

У к а з а н и е. Задача равносильна следующей: существует ли многочлен $f(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1}$, у которого коэффициенты являются перестановкой последовательности $1, \dots, n$, такой, что $f(\varepsilon_n) = 0$, где $\varepsilon_n = e^{2\pi i/n}$? Примените задачи 24, 25 и 29.

Если $(m, n) = 1$, то

$$\begin{aligned} (1 + 2x + \dots + nx^{n-1})(1 + x^n + x^{2n} + \dots + x^{(m-1)n}) + \\ + (nx + \dots + n(m-1)x^{m-1})(1 + x^m + x^{2m} + \dots + x^{(n-1)m}) = \\ = a_0 + a_1x + \dots + a_{mn-1}x^{mn-1}, \end{aligned}$$

где числа последовательности a_k дают при делении на n и m разные пары остатков, так как остатки по модулю n повторяются с периодом n , а остатки по модулю m повторяются с периодом m , и оба периода состоят из разных чисел, поэтому, согласно китайской теореме, все числа последовательности a_k будут разными по модулю mn , а значит, образуют перестановку последовательности $1, \dots, mn$.

§ 4.6. Кубические уравнения над полем комплексных чисел

Тригонометрическая форма записи комплексного числа позволяет установить связь между решениями уравнения третьей степени из предыдущих параграфов. Для этого вернемся к нашему уравнению

$$(u^3)^2 + Bu^3 - \frac{A^3}{27} = 0.$$

Пусть

$$\Delta = \frac{A^3}{27} + \frac{B^2}{4} < 0.$$

Тогда

$$u^3 = -\frac{B}{2} \pm \sqrt{|\Delta|}i, \quad v^3 = -\frac{B}{2} \mp \sqrt{|\Delta|}i$$

— сопряженные друг другу комплексные числа.

Нам нужно извлечь из них корень третьей степени.

Определение 100. Назовем *корнем n -й степени* из комплексного числа z и обозначим $\sqrt[n]{z}$ множество всех комплексных чисел, при возведении в n -ю степень дающих z .

Из теоремы 97 следует, что этих чисел n штук и что они имеют следующий вид:

$$\sqrt[n]{|z|} \left(\cos \frac{\varphi + 2k\pi}{n} + i \sin \frac{\varphi + 2k\pi}{n} \right) \quad \text{при } k = 0, 1, \dots, n-1.$$

В силу того, что $u^{-3} = (\bar{v})^{-3}$, можно считать, что числа u и v сопряжены. Значит, их сумма вещественна. Это означает, что мы получили три вещественных решения уравнения $x^3 + Ax + B = 0$ в виде

$$u + v = \sqrt[3]{-\frac{B}{2} + \sqrt{\Delta}} + \sqrt[3]{-\frac{B}{2} - \sqrt{\Delta}}.$$

Упражнение 101. Выведите из этой формулы тригонометрическое решение кубического уравнения.

Полученное выражение может иметь, вообще говоря, 36 значений: каждый из двух радикалов $\sqrt[3]{}$ принимает по 3 значения и каждый из двух радикалов $\sqrt{}$ принимает по 2 значения. А нам нужны только три из них.

С квадратными радикалами справиться легко, так как извлекается корень из одного и того же выражения Δ . Для этого условимся, что если в некоторой формуле несколько раз встречается радикал из одного и того же выражения, то этому радикалу придается одно и то же значение. Наше выражение $u + v$ не меняется при одновременной смене знака у $\sqrt{\Delta}$ в двух местах. Поэтому остается лишь 9 значений для корней, зависящих от выбора значений двух радикалов 3-й степени.

Для устранения этой трудности заметим, что второе уравнение системы из предыдущего параграфа имеет вид $uv = -\frac{A}{3}$, т. е. произведение uv всегда действительно. Выберем произвольное значение u_1 . Тогда из формулы для произведения комплексных чисел в тригонометрической форме следует, что все другие значения u_1 суть $u_1\rho$ и $u_1\rho^2$, где

$$\rho = \cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$$

(напомним, что $\rho^3 = 1$). Каждому значению $u = u_1, u_1\rho, u_1\rho^2$ сопоставим $v = -\frac{A}{3u}$. Тогда v принимает значения $v_1, v_1\rho^2, v_1\rho$.

В результате доказана

Теорема 98. Все вещественные корни уравнения

$$x^3 + Ax + B = 0$$

при вещественных A и B находятся среди трех чисел:

$$x_1 = u_1 + v_1; \quad x_2 = u_1\rho + v_1\rho; \quad x_3 = u_1\rho^2 + v_1\rho^2, \quad (3)$$

где u_1 — произвольное из значений корня

$$\sqrt[3]{-\frac{B}{2} + \sqrt{\Delta}},$$

$$\text{а } v_1 = -\frac{A}{3u_1}.$$

Причем если $\Delta > 0$, то ровно одно из них вещественно, если $\Delta < 0$, то все три числа вещественны.

Сделаем теперь следующий шаг в обобщении: будем считать коэффициенты исходного уравнения комплексными числами. При решении ничего по сути не меняется: мы приходим к системе, решая которую, получаем формулу для корней кубического уравнения в радикалах. Три корня определяем, как и выше: выбираем произвольно u_1 , потом берем $v_1 = -\frac{A}{3u_1}$ и выписываем формулы (3).

Тогда получаем комплексный вариант формулы Кардано:

Теорема 99. Все корни уравнения

$$x^3 + Ax + B = 0$$

при произвольных комплексных A и B задаются формулами

$$x_1 = u_1 + v_1, \quad x_2 = u_1\rho + v_1\rho, \quad x_3 = u_1\rho^2 + v_1\rho^2,$$

где u_1 — произвольное из значений корня

$$\sqrt[3]{-\frac{B}{2} + \sqrt{\Delta}},$$

$$\text{а } v_1 = -\frac{A}{3u_1}.$$

Легко видеть из формул для решения кубического уравнения, что $\Delta = 0$ тогда и только тогда, когда у исходного уравнения есть кратные корни.

В дальнейшем, если не оговорено противное, мы будем считать коэффициенты алгебраических уравнений комплексными числами.

Задачи и упражнения к § 4.6

1. Докажите, что при решении уравнений с рациональными коэффициентами по формуле Кардано все корни в формуле извлекаются тогда и только тогда, когда решения уравнения имеют вид $2a$, $-a \mp bi\sqrt{3}$ при рациональных a и b .

2. Докажите, что

$$\sqrt[3]{a+bi} = \frac{u(a+bi) + u^2i}{2a\sqrt[3]{a^2+b^2}},$$

где u — корень уравнения $u^3 - 3(a^2 + b^2)u - 2b(a^2 + b^2) = 0$.

3. Решите по формуле Кардано уравнения:

- а) $x^3 - 6x + 9 = 0$; д) $x^3 + 6x + 2 = 0$;
 б) $x^3 + 12x + 63 = 0$; е) $x^3 + 3x^2 - 6x + 4 = 0$;
 в) $x^3 + 9x^2 + 18x + 28 = 0$; ж) $x^3 + 3x - 2i = 0$;
 г) $x^3 + 6x^2 + 30x + 25 = 0$; з) $x^3 - 3ax + a^3 + 1 = 0$.

4. Если все корни уравнения $z^3 + az^2 + bz + c = 0$ по модулю равны 1, то модули a и b равны.

§ 4.7. Уравнения четвертой степени

Общее уравнение четвертой степени имеет вид:

$$x^4 + ax^3 + bx^2 + cx + d = 0.$$

Как и раньше, уничтожим коэффициент a , выделяя полную четвертую степень. Для этого сделаем замену переменной $x' = x + a/4$.

Упражнение 102. Проверьте, что после этой замены уравнение примет вид $x^4 + Ax^2 + Bx + C = 0$.

Попробуем разложить его в произведение двух квадратных уравнений:

$$x^4 + Ax^2 + Bx + C = (x^2 + u_1x + v_1)(x^2 + u_2x + v_2).$$

Раскрывая скобки и приравнявая коэффициенты, получаем систему

$$\begin{cases} u_1 + u_2 = 0; \\ v_1 + v_2 + u_1u_2 = A; \\ u_1v_2 + u_2v_1 = B; \\ v_1v_2 = C. \end{cases}$$

Заменяя u_2 на $-u_1 = -u$, приходим к системе с тремя неизвестными:

$$\begin{cases} v_1 + v_2 = A + u^2; \\ u(v_2 - v_1) = B; \\ v_1v_2 = C, \end{cases}$$

которая равносильна системе

$$\begin{cases} v_1 + v_2 = A + u^2; \\ v_2 - v_1 = \frac{B}{u}; \\ v_1 v_2 = C, \end{cases}$$

а последняя — системе

$$\begin{cases} 2v_2 = A + u^2 + \frac{B}{u}; \\ 2v_1 = A + u^2 - \frac{B}{u}; \\ 4v_1 v_2 = 4C. \end{cases}$$

Отсюда имеем

$$4C = 4v_1 v_2 = \left((A + u^2) + \frac{B}{u} \right) \left((A + u^2) - \frac{B}{u} \right) = (A + u^2)^2 - \frac{B^2}{u^2},$$

или

$$u^6 + 2Au^4 + (A^2 - 4C)u^2 - B^2 = 0.$$

Решив это кубическое относительно u^2 уравнение, называемое *резольвентой Феррари**, найдем решения системы. После этого, решив два квадратных уравнения, получим решения уравнения 4-й степени.

Задачи и упражнения к § 4.7

1. Выразите через корни уравнения четвертой степени корни его резольвенты Феррари.

2. Решите уравнения

а) $x^4 - 2x^3 + 2x^2 + 4x - 8 = 0$;	д) $x^4 - 3x^3 + x^2 + 4x - 6 = 0$;
б) $x^4 + 2x^3 - 2x^2 + 6x - 15 = 0$;	е) $x^4 - 2x^3 + 4x^2 - 2x + 3 = 0$;
в) $x^4 - x^3 - x^2 + 2x - 2 = 0$;	ж)* $4x^4 + 12x^2 + 16x - 3 = 0$;
г) $x^4 - 4x^3 + 3x^2 + 2x - 1 = 0$;	з)* $4x^4 + 4x + 3 = 0$.

§ 4.8. Решение кубического уравнения методом Лагранжа

Приведенные выше решения уравнений 2, 3 и 4-й степени оставляют чувство неудовлетворенности. Создается впечатление, что они найдены при помощи искусственных, не обобщаемых на высшие степени, приемов. В какой-то мере это действительно так. Однако можно предложить

* Л. Феррари (Lodovico Ferrari, 1522–1565) — итальянский математик, ученик Кардано, первым решивший уравнение четвертой степени.

Пусть $x_1, \dots, x_n$ — все корни уравнения

Упражнение 103. Вспомните, как доказываются формулы Виета (здесь мы уже можем считать, что корни уравнения — произвольные комплексные числа)

[illegible]

$$\begin{cases} u + v = a; \\ uv = b. \end{cases}$$

Прежде всего заметим, что сумма $x_1 + x_2 + x_3$ равна нулю (так как она отличается от коэффициента при x^2 исходного уравнения лишь знаком).

Пусть $\rho = -\frac{1}{2} + \frac{\sqrt{-3}}{2}$ — корень третьей степени из единицы.

Напишем еще две суммы:

$$(\rho, x) = x_1 + \rho x_2 + \rho^2 x_3 \quad \text{и} \quad (\rho, x) = x_1 + \rho^2 x_2 + \rho x_3.$$

$$x_2 + \rho x_3 + \rho^2 x_1 = \rho^2(\rho, x), \quad x_2 + \rho x_1 + \rho^2 x_3 = \rho(\rho^2, x) \quad \text{и т. д.}$$

Кроме того, меняя местами пару переменных одной из сумм в (ρ, x) и (ρ^2, x) , получим выражение, пропорциональное другой сумме:

$$x_2 + \rho x_1 + \rho^2 x_3 = \rho(\rho^2, x), \quad x_2 + \rho^2 x_1 + \rho x_3 = \rho^2(\rho, x) \quad \text{и т. д.}$$

При указанных заменах переменных коэффициенты пропорциональности всегда суть корни третьей степени из единицы, так что при возведении в куб они равны единице. Поэтому выражение $(\rho, x)^3 + (\rho^2, x)^3$ не меняется при перестановках переменных.

Отметим, что коэффициенты пропорциональности у выражений (ρ, x) и (ρ^2, x) при одной и той же перестановке переменных взаимно обратны. Поэтому выражение $(\rho, x) \cdot (\rho^2, x)$ также не меняется при заменах переменных.

Выразим их через коэффициенты a и b . Прежде всего заметим, что

$$(\rho, x)^3 + (\rho^2, x)^3 = ((\rho, x) + (\rho^2, x))((\rho, x) + (\rho^2, x))^2 - 3(\rho, x)(\rho^2, x),$$

$$\begin{aligned} (\rho, x) + (\rho^2, x) &= (x_1 + \rho x_2 + \rho^2 x_3) + (x_1 + \rho^2 x_2 + \rho x_3) = \\ &= 2x_1 + (\rho + \rho^2)(x_2 + x_3) = 2x_1 - (x_2 + x_3) = \\ &= 3x_1 - (x_1 + x_2 + x_3) = 3x_1 - 0 = 3x_1 \end{aligned}$$

(так как $\rho + \rho^2 = -1$) и

$$\begin{aligned} (\rho, x)(\rho^2, x) &= (x_1 + \rho x_2 + \rho^2 x_3)(x_1 + \rho^2 x_2 + \rho x_3) = x_1^2 + x_2^2 + x_3^2 + \\ &+ (\rho + \rho^2)(x_1 x_2 + x_2 x_3 + x_3 x_1) = x_1 + x_2 + x_3 - (x_1 x_2 + x_2 x_3 + x_3 x_1) = \\ &= (x_1 + x_2 + x_3)^2 - 3(x_1 x_2 + x_2 x_3 + x_3 x_1) = 0 - 3a = -3a \end{aligned}$$

(так как $x_1 + x_2 + x_3 = 0$).

Поэтому

$$(\rho, x)^3 + (\rho^2, x)^3 = 3x_1(9x_1^2 + 9a) = 27(x_1^3 + ax_1).$$

Однако x_1 — корень исходного уравнения, значит, $x_1^3 + ax_1 + b = 0$, откуда $x_1^3 + ax_1 = -b$.

Поэтому в результате получаем, что

$$\begin{cases} (\rho, x)^3 + (\rho^2, x)^3 = -27b; \\ (\rho, x) \cdot (\rho^2, x) = -3a. \end{cases}$$

Полученная система легко решается относительно неизвестных (ρ, x) и (ρ^2, x) . Действительно,

$$(\rho^2, x) = \frac{-3a}{(\rho, x)},$$

поэтому

$$(\rho, x)^6 + 27b(\rho, x)^3 - 27a^3 = 0,$$

значит,

$$\begin{cases} (\rho, x)^3 = 27\left(-\frac{b}{2} + \sqrt{\Delta}\right); \\ (\rho^2, x)^3 = 27\left(-\frac{b}{2} - \sqrt{\Delta}\right), \end{cases} \quad (4)$$

где

$$\Delta = \frac{a^3}{27} + \frac{b^2}{4},$$

или

$$\begin{cases} (\rho, x)^3 = 27A; \\ (\rho^2, x)^3 = 27B, \end{cases}$$

где

$$A = -\frac{b}{2} + \sqrt{\Delta}, \quad B = -\frac{b}{2} - \sqrt{\Delta}.$$

Выразим x_1, x_2, x_3 из (ρ, x) и (ρ^2, x) , последовательно исключая неизвестные из системы:

$$\begin{cases} x_1 + x_2 + x_3 = 0; \\ x_1 + \rho x + \rho^2 x = 3\sqrt[3]{A}; \\ x_1 + \rho^2 x + \rho x = 3\sqrt[3]{B}. \end{cases}$$

Складывая все три уравнения с учетом равенства $1 + \rho + \rho^2 = 0$ и сокращая тройку, находим

$$x_1 = \sqrt[3]{A} + \sqrt[3]{B}.$$

Аналогично, умножая второе уравнение на ρ^2 , третье на ρ и складывая их с первым, после сокращения на три находим

$$x_2 = \rho^2 \sqrt[3]{A} + \rho \sqrt[3]{B}.$$

А умножая второе уравнение на ρ , третье на ρ^2 и складывая их с первым, имеем

$$x_3 = \rho \sqrt[3]{A} + \rho^2 \sqrt[3]{B}.$$

В результате мы получили формулы Кардано (3) из теоремы 98 с точностью до порядка следования x_1, x_2, x_3 .

Из этих формул вытекает выражение

$$\begin{aligned} ((\rho, x)^3 - (\rho^2, x)^3)^2 &= ((\rho, x)^3 + (\rho^2, x)^3)^2 - 4(\rho, x)^3(\rho^2, x)^3 = \\ &= (-27b)^2 + 4(27a^3) = 27(4a^3 + 27b^2) = 27 \cdot 108\Delta. \end{aligned}$$

Упражнение 106. Выведите из предыдущего равенства, что

$$108\Delta = (x_2 - x_1)^2(x_3 - x_2)^2(x_3 - x_1)^2,$$

используя равенства

$$u^3 - v^3 = (u - v)(u - \rho v)(u - \rho^2 v), \quad (1 - \rho)(1 - \rho^2) = 3.$$

Определение 101. Выражение

$$D = (x_2 - x_1)^2(x_3 - x_2)^2(x_3 - x_1)^2$$

называют *дискриминантом кубического уравнения*.

Вообще, *дискриминантом уравнения n -й степени*

$$x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0$$

называют симметрический многочлен от корней $x_1, x_2, \dots, x_n$ этого уравнения $D = \prod_{i>j} (x_i - x_j)^2$.

Задачи и упражнения к § 4.8

1. Выразить дискриминант D через коэффициенты для общего уравнения третьей и четвертой степени.

2. Решите общее уравнение третьей степени в случае нулевого дискриминанта.

3*. Решите уравнение

$$(x^3 - 3qx + p^3 - 3pq)^2 - 4(px + q)^3 = 0.$$

У к а з а н и е. Рассмотрите уравнение относительно z

$$z^3 - (3px + q)z + x^3 - 3qx + p^3 - 3pq = 0$$

с нулевым дискриминантом и вынесите в нем за скобки множитель $z + x + p$.

4. Решите уравнения:

а) $(x^2 + 3)/(x + 3)^3 = 26/343$; б) $x^6 + 1 = 0$; в) $(x^2 + x)^4 = 1$.

5. Числа a, b, c — три из четырех корней многочлена $x^4 - ax^3 - bx + c$. Найдите эти числа.

6. Найдите все p и q , при которых четыре корня многочлена $x^4 + px^2 + q$ действительны и образуют арифметическую прогрессию.

§ 4.9. Решение методом Лагранжа уравнений четвертой степени

Попытаемся обобщить метод предыдущего параграфа на случай 4-й степени. Рассмотрим выражение

$$t(x_1, x_2, x_3, x_4) = x_1 + \alpha x_2 + \alpha^2 x_3 + \alpha^3 x_4,$$

где $\alpha = i$ — корень 4-й степени из 1, а $x_1, \dots, x_4$ — корни уравнения $x^4 + ax^2 + bx + c = 0$, то есть

$$t = x_1 - x_3 + (x_2 - x_4)i.$$

Сколько значений принимает выражение t при различных перестановках корней? Очевидно, 24 значения — столько же, сколько всех возможных перестановок.

Однако заметим, что некоторые перестановки дают выражения, пропорциональные t , причем коэффициенты пропорциональности являются корнями четвертой степени из 1.

Это происходит при циклической перестановке $\Pi = x_1 \rightarrow x_2 \rightarrow x_3 \rightarrow x_4 \rightarrow x_1$ и, следовательно, еще при двух перестановках, являющихся ее степенями, а именно при перестановках Π^2, Π^3 (перестановка Π^4 уже является тождественной). Можно это проверить и непосредственно, например, заметив, что перестановка Π^2 меняет местами переменные x_1 и x_3 , а также переменные x_2 и x_4 , и выражение t при этом меняет знак на противоположный.

Заметим, что при этих перестановках выражение t^4 вообще не меняется.

Упражнение 107. Проверьте, что любая другая перестановка не обладает этим свойством.

Упражнение 108. Проверьте, что при всех 24 перестановках выражение t^4 принимает ровно $24/4 = 6$ значений:

$$\begin{aligned} t_1^4 &= [(x_1 - x_2) + (x_3 - x_4)i]^4; & t_2^4 &= [(x_1 - x_3) + (x_2 - x_4)i]^4; \\ t_3^4 &= [(x_1 - x_4) + (x_2 - x_3)i]^4; & t_4^4 &= [(x_1 - x_2) + (x_4 - x_3)i]^4; \\ t_5^4 &= [(x_1 - x_3) + (x_4 - x_2)i]^4; & t_6^4 &= [(x_1 - x_4) + (x_3 - x_2)i]^4. \end{aligned}$$

Эти значения являются корнями уравнения шестой степени, коэффициенты которого полиномиально выражаются через коэффициенты исходного уравнения. Получившееся уравнение шестой степени можно разложить на два кубических. Однако этот способ требует слишком много вычислений.

Попытаемся найти более удобные выражения, чем $t(x_1, x_2, x_3, x_4)$. Для этого рассмотрим подробнее метод разложения на два множителя, примененный Феррари.

Его идея состоит в том, чтобы представить левую часть уравнения $x^4 + ax^3 + bx^2 + cx + d = 0$ в виде разности двух квадратов. Тогда ее можно будет разложить на два множителя второй степени, и решение уравнения приведет к решению двух квадратных уравнений. Для этого левую часть представим в виде

$$\begin{aligned} \left(x^2 + \frac{a}{2}x + \frac{y}{2}\right)^2 - \frac{a^2}{4}x^2 - \frac{ayx}{2} - \frac{y^2}{4} - yx^2 + bx^2 + cx + d = \\ = \left(x^2 + \frac{a}{2}x + \frac{y}{2}\right)^2 - \left[\left(\frac{a^2}{4} + y - b\right)x^2 + \left(\frac{ay}{2} - c\right)x + \left(\frac{y^2}{4} - d\right)\right], \end{aligned}$$

где y — вспомогательная неизвестная, которую подберем так, чтобы выражение в квадратных скобках оказалось квадратом линейного двучлена.

Для этого необходимо и достаточно выполнения условия

$$\left(\frac{ay}{2} - c\right)^2 - 4\left(\frac{a^2}{4} + y - b\right)\left(\frac{y^2}{4} - d\right) = 0.$$

Это условие есть кубическое уравнение относительно y . Оно называется *резольвентой Феррари*.

После раскрытия скобок уравнение преобразуется к виду

$$y^3 - by^2 + (ac - 4d)y - (c^2 + a^2d - 4bd) = 0.$$

Пусть y_1 — один из корней этого уравнения. Тогда при $y = y_1$ условие будет выполнено, так что имеет место

$$\left(\frac{a^2}{4} + y_1 - b\right)x^2 + \left(\frac{ay_1}{2} - c\right)x + \left(\frac{y_1^2}{4} - d\right) = (kx + l)^2$$

при некоторых k и l . Исходное уравнение примет вид

$$\left(x^2 + \frac{a}{2}x + \frac{y_1}{2}\right)^2 - (kx + l)^2 = 0,$$

или

$$\left(x^2 + \frac{a}{2}x + \frac{y_1}{2} + kx + l\right) \cdot \left(x^2 + \frac{a}{2}x + \frac{y_1}{2} - kx - l\right) = 0.$$

Приравняв к нулю каждый из сомножителей, находим четыре корня исходного уравнения.

Пусть x_1 и x_2 — корни первого сомножителя, x_3 и x_4 — корни второго. Тогда $x_1x_2 = \frac{y_1}{2} + l$, $x_3x_4 = \frac{y_1}{2} - l$. Сложив эти равенства, получим, что $y_1 = x_1x_2 + x_3x_4$. Таким образом, мы получим выражение корня y_1 вспомогательного кубического уравнения через корни исходного уравнения четвертой степени.

Другими корнями кубического уравнения будут

$$y_2 = x_2x_3 + x_1x_4, \quad y_3 = x_2x_4 + x_1x_3.$$

Таким образом, мы нашли такое выражение $y_1 = x_1x_2 + x_3x_4$ от корней x_1 , x_2 , x_3 , x_4 , что при их всевозможных перестановках получается только два новых выражения. Поэтому эти выражения являются корнями уравнения третьей степени, коэффициенты которого полиномиально выражаются через коэффициенты исходного уравнения четвертой степени.

Данный результат можно было получить и двигаясь от этих выражений к уравнению третьей степени.

Действительно, $y_1 + y_2 + y_3 = \sum x_i x_j = b$ согласно теореме Виета для уравнения $x^4 + ax^3 + bx^2 + cx + d = 0$.

Аналогично

$$\begin{aligned} y_1 y_2 + y_2 y_3 + y_3 y_1 &= x_1^2 x_2 x_3 + x_1 x_2^2 x_4 + x_1 x_3^2 x_4 + x_2 x_3 x_4^2 + \dots = \\ &= (x_1 + x_2 + x_3 + x_4)(x_1 x_2 x_3 + x_1 x_3 x_4 + x_2 x_3 x_4 + x_1 x_2 x_4) - 4x_1 x_2 x_3 x_4 = \\ &= ac - 4d \end{aligned}$$

и также

$$\begin{aligned} y_1 y_2 y_3 &= (x_1^3 x_2 x_3 x_4 + x_1 x_2^3 x_3 x_4 + x_1 x_2 x_3^3 x_4 + x_1 x_2 x_3 x_4^3) + \\ &\quad + (x_1^2 x_2^2 x_3^2 + x_1^2 x_2^2 x_4^2 + x_1^2 x_3^2 x_4^2 + x_2^2 x_3^2 x_4^2) = \\ &= x_1 x_2 x_3 x_4 (x_1^2 + x_2^2 + x_3^2 + x_4^2)^2 + (x_1 x_2 x_3 + x_1 x_2 x_4 + x_1 x_2 x_3 + x_2 x_3 x_4)^2 - \\ &\quad - 2(x_1 x_2 + x_1 x_3 + x_1 x_4 + x_2 x_3 + x_2 x_4 + x_3 x_4) x_1 x_2 x_3 x_4 = \\ &= d(a^2 - 2b) + (c^2 - 2bd) = c^2 + a^2 d - 4bd. \end{aligned}$$

Значит, y_1, y_2, y_3 — корни уравнения

$$y^3 - by^2 + (ca - 4d)y - (c^2 + a^2 d - 4bd) = 0.$$

После решения этого уравнения остается справиться с системой

$$\begin{cases} x_1 x_2 + x_3 x_4 = y_1; \\ x_1 x_3 + x_2 x_4 = y_2; \\ x_1 x_4 + x_2 x_3 = y_3. \end{cases}$$

Упражнение 109. Решите эту систему.

Рассмотрим еще один метод решения уравнения 4-й степени $x^4 + ax^2 + bx + c = 0$.

Возьмем другое выражение от корней x_1, x_2, x_3, x_4 , которое тоже принимает при переставлении корней всего 3 значения:

$$\theta_1 = (x_1 + x_2)(x_3 + x_4), \quad \theta_2 = (x_1 + x_3)(x_2 + x_4), \quad \theta_3 = (x_1 + x_4)(x_2 + x_3).$$

Найдем кубическое уравнение с корнями $\theta_1, \theta_2, \theta_3$. Другими словами, выразим его коэффициенты $A = -\theta_1 - \theta_2 - \theta_3, B = \theta_1 \theta_2 + \theta_2 \theta_3 + \theta_3 \theta_1, C = -\theta_1 \theta_2 \theta_3$ через коэффициенты a, b, c :

$$\begin{aligned} \theta_1 + \theta_2 + \theta_3 &= 2(x_1 x_2 + x_3 x_4 + x_2 x_3 + x_1 x_3 + x_1 x_4 + x_2 x_4) = 2a, \\ \theta_1 \theta_2 + \theta_2 \theta_3 + \theta_3 \theta_1 &= a^2 - 4c, \quad \theta_1 \theta_2 \theta_3 = -b^2. \end{aligned}$$

Используя теорему Виета, имеем

$$(x - \theta_1)(x - \theta_2)(x - \theta_3) = x^3 - 2ax^2 + (a - 4c)x + b^2.$$

Найдя из этого уравнения $\theta_1, \theta_2, \theta_3$, можно определить и корни x_1, x_2, x_3, x_4 . Для этого используем равенство $x_1 + x_2 + x_3 + x_4 = 0$, из которого следует, что $(x_1 + x_2) = -(x_3 + x_4), (x_1 + x_3) = -(x_2 + x_4), (x_1 + x_4) = -(x_2 + x_3)$.

Значит,

$$x_1 + x_2 = \sqrt{-\theta_1}; \quad x_3 + x_4 = -\sqrt{-\theta_1};$$

$$x_1 + x_3 = \sqrt{-\theta_2}; \quad x_2 + x_4 = -\sqrt{-\theta_2};$$

$$x_1 + x_4 = \sqrt{-\theta_3}; \quad x_2 + x_3 = \sqrt{-\theta_3}.$$

Отсюда можно выразить x_1, x_2, x_3, x_4 .

Упражнение 110. Сделайте это.

Любопытно, что дискриминант найденного выше кубического уравнения равен дискриминанту уравнения 4-й степени для x . В самом деле,

$$\theta_1 - \theta_2 = -(x_1 - x_4)(x_2 - x_3);$$

$$\theta_1 - \theta_3 = -(x_1 - x_3)(x_2 - x_4);$$

$$\theta_2 - \theta_3 = -(x_1 - x_2)(x_3 - x_4).$$

Упражнение 111. Вычислите этот дискриминант.

Задачи и упражнения к § 4.9

1. Решите биквадратное уравнение методом Лагранжа.
2. Решите уравнения:
 - а) $x^4 - 2(a^2 + b^2)x^2 + (a^2 - b^2)^2 = 0$;
 - б) $x^4 - a(a + b)x^2 + a^3b = 0$;
 - в) $(x^2 + 1)^2 = 4(2x - 1)$;
 - г) $(x^2 - 16)(x - 3)^2 + 9x^2 = 0$;
 - д) $x^4 - 12x + 323 = 0$;
 - е) $(6x + 5)^2(3x + 2)(x + 1) = 35$;
 - ж) $x^4 + x^3 + x + 1 = 4x^2$;
 - з) $(1 + x)^4 = 2(1 + x)^4$;
 - и) $45(x^2 + x + 1)^2 = 49(x + 1)^2(x + 1)^2$;
 - к) $(x^2 - 10x + 15)(x^2 - 8x + 15) = 3(x^2 - 6x + 15)x$.
3. Составить уравнение 4-й степени с корнями $\alpha, 1/\alpha, -\alpha, -1/\alpha$.
4. Пусть a и b — два из четырех корней многочлена $x^4 + x^3 - 1$. Покажите, что ab — корень многочлена $x^6 + x^4 + x^3 - x^2 - 1$.

§ 4.10. Решение методом Эйлера уравнений четвертой степени

Существуют и другие способы решения уравнения четвертой степени. Один из наиболее изящных принадлежит Эйлеру. Этот способ состоит в следующем.

Полное уравнение четвертой степени

$$y^4 + Ay^3 + By^2 + Cy + D = 0 \quad (5)$$

подстановкой $y = x - \frac{A}{4}$ приводится к более простому виду:

$$x^4 + ax^2 + bx + c = 0. \quad (6)$$

Полагаем:

$$2x = u + v + w. \quad (7)$$

В равенство (7) введено три неизвестных. Чтобы определить их, нужно будет дать три уравнения.

Возводя обе части равенства (7) два раза в квадрат, получаем:

$$\begin{aligned} 4x^2 &= u^2 + v^2 + w^2 + 2(uv + uw + vw), \\ 16x^4 &= (u^2 + v^2 + w^2)^2 + 4(uv + uw + vw)(u^2 + v^2 + w^2) + \\ &\quad + 4(u^2v^2 + u^2w^2 + v^2w^2) + 8uvw(u + v + w). \end{aligned} \quad (8)$$

Подставляя в уравнение (6) вместо x , x^2 и x^4 их выражения из равенств (7) и (8), после упрощения получим:

$$\begin{aligned} (u^2 + v^2 + w^2)^2 + 4(uv + uw + vw)(u^2 + v^2 + w^2 + 2a) + \\ + 4a(u^2 + v^2 + w^2) + 8(uvw + b)(u + v + w) + \\ + 4(u^2v^2 + u^2w^2 + v^2w^2) + 16c = 0. \end{aligned} \quad (9)$$

Для того чтобы выполнялось равенство $2x = u + v + w$, где x — корень уравнения (6), необходимо и достаточно выполнение уравнения (9). Оно содержит три неизвестных. Чтобы определить их, нужны еще два уравнения, которые можно выбрать произвольно. Свободой выбора следует воспользоваться для наибольшего упрощения уравнения.

Руководствуясь этим, положим

$$u^2 + v^2 + w^2 = -2a; \quad uvw = -b. \quad (10)$$

При этом выборе величин u , v и w уравнение (9) обращается в уравнение

$$u^2v^2 + u^2w^2 + v^2w^2 = a - 4c. \quad (11)$$

Из (10) и (11) заключаем, что u , v и w удовлетворяют системе уравнений

$$\begin{cases} u^2 + v^2 + w^2 = -2a; \\ u^2v^2 + u^2w^2 + v^2w^2 = a^2 - 4c; \\ u^2v^2w^2 = b^2. \end{cases} \quad (12)$$

Отсюда следует, что числа u^2 , v^2 и w^2 являются корнями уравнения:

$$\sigma^3 + 2a\sigma^2 + (a^2 - 4c) - b^2 = 0. \quad (13)$$

Оно совпадает с резольвентой Феррари, полученной ранее.

Пусть σ_1 , σ_2 , σ_3 — корни резольвенты. Положим $u^2 = \sigma_1$, $v^2 = \sigma_2$, $w^2 = \sigma_3$. Извлекая корни, имеем

$$u = \pm\sqrt{\sigma_1}, \quad v = \pm\sqrt{\sigma_2}, \quad w = \pm\sqrt{\sigma_3}. \quad (14)$$

При этом, в силу равенства (10), выполняется равенство

$$(\pm\sqrt{\sigma_1}) \cdot (\pm\sqrt{\sigma_2}) \cdot (\pm\sqrt{\sigma_3}) = -b. \quad (15)$$

У двух радикалов в равенствах (14) можно взять любое из их значений. После этого значение третьего радикала следует взять определенное — оно находится из равенства (15).

Подставляя полученные выражения для u , v , w в уравнение (7), приходим к следующей теореме.

Теорема 100 (Эйлер). *Корни приведенного уравнения четвертой степени*

$$x^4 + ax^2 + bx + c = 0$$

выражаются через корни резольвенты Феррари

$$\sigma^3 + 2a\sigma^2 + (a^2 - 4c)\sigma - b^2 = 0$$

по формулам:

$$\begin{aligned} 2x_1 &= \sqrt{\sigma_1} + \sqrt{\sigma_2} + \sqrt{\sigma_3}; & 2x_2 &= \sqrt{\sigma_1} - \sqrt{\sigma_2} - \sqrt{\sigma_3}; \\ 2x_3 &= -\sqrt{\sigma_1} + \sqrt{\sigma_2} - \sqrt{\sigma_3}; & 2x_4 &= -\sqrt{\sigma_1} - \sqrt{\sigma_2} + \sqrt{\sigma_3}. \end{aligned}$$

При этом значения радикалов $\sqrt{\sigma_1}$, $\sqrt{\sigma_2}$ и $\sqrt{\sigma_3}$ должны быть выбраны так, чтобы выполнялось равенство:

$$\sqrt{\sigma_1} \cdot \sqrt{\sigma_2} \cdot \sqrt{\sigma_3} = -b.$$

Задачи и упражнения к § 4.10

1. Решите биквадратное уравнение методом Эйлера.

2. Решите уравнения:

а) $x^4 + 2x + \frac{3}{2} = 0$;

б) $x^4 - \frac{17}{2}x^2 + 10x - \frac{31}{16} = 0$;

в) $x^4 - 12x^2 - 24x - 14 = 0$.

3. Разложите на множители над полем действительных чисел

а) $(x^2 + x + 4)^2 + 8x(x^2 + x + 4)^2 + 15x$;

б) $(x + 1)(x + 3)(x + 5)(x + 7) + 15$;

в) $4(x + 5)(x + 6)(x + 10)(x + 12) - 3x^2$;

г) $x^4 + 4$;

д) $x^4 + 4x^2 + 4x + 1$.

§ 4.11. Основная теорема алгебры

Важным шагом в развитии теории алгебраических уравнений стало использование комплексных чисел в качестве коэффициентов уравнений. В 1799 г. Гаусс дал первое строгое доказательство существования комплексных решений для любого алгебраического уравнения (этот факт был известен и ранее и был доказан Даламбером *, правда, с некоторым промахом).

Теорема 101 (Даламбер–Гаусс). *Всякий многочлен степени $n \geq 1$ имеет комплексный корень.*

Доказательство. Для понимания идеи одного из самых наглядных доказательств этой теоремы можно предложить следующие неформальные рассуждения. Это доказательство, носящее название «Дама с собачкой», рассказывалось А. Н. Колмогоровым в 1930-е годы на лекции для школьников в МГУ.

Рассмотрим многочлен $f(z) = z^n + a_1 z^{n-1} + \dots + a_n$ с комплексными коэффициентами и $a_n \neq 0$. Заметим, что все его корни (если они существуют) лежат в круге радиуса $R = n \cdot \max_i |a_i|$. Действительно, при $|z| > R$

$$|z^n| > |a_1 z^{n-1} + \dots + a_n|,$$

и поэтому $f(z) \neq 0$. В тоже время при малых по модулю z значение $f(z)$ близко к a_n .

Представим $f(z)$ в виде суммы двух частей z^n и $g(z) = a_1 z^{n-1} + \dots + a_n$, которые назовем соответственно «дамой» и «собачкой». Рассмотрим образы окружностей различных радиусов с центрами в точке O при отображении $f(z)$ (рис. 34).

Для радиуса R при движении по окружности

$$\{R(\cos \varphi + i \sin \varphi) : 0 \leq \varphi \leq 2\pi\}$$

* Ж. Л. Даламбер (Jean Le Rond d'Alembert, 1717–1783) — выдающийся французский математик и механик, один из организаторов издания знаменитой «Энциклопедии».

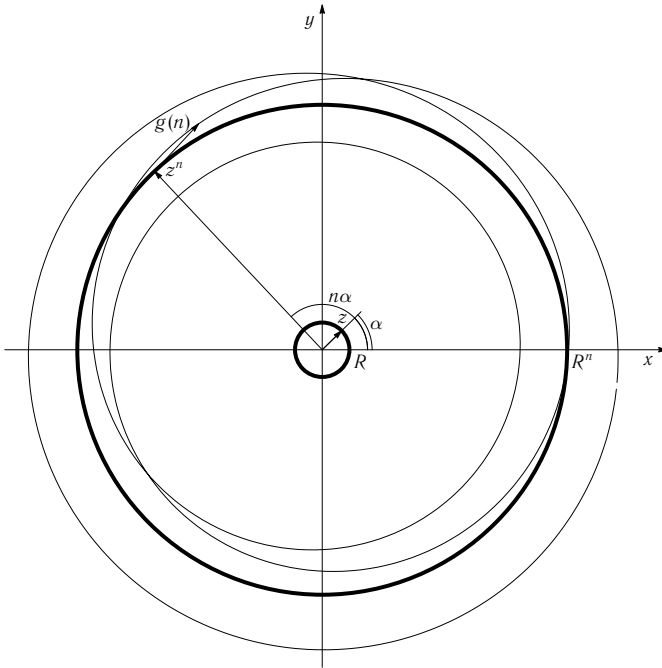


Рис. 34

дама будет двигаться в образе со скоростью, в n раз большей, по окружности радиуса R^n . Собачка $g(z) = f(z) - z^n$ будет мала по модулю и не заденет за точку $(0, 0)$, как было показано выше. При малых радиусах образ будет «бегать» неподалеку от точки $a_n \neq 0$.

Начнем непрерывно уменьшать радиус окружности от R до 0 . В начале точка $(0, 0)$ была внутри, а в конце стала находиться вне множества, ограниченного образом окружности. В силу непрерывности будет момент прохождения через эту точку. Это означает, что в этот момент $f(z) = 0$, т. е. у многочлена $f(z)$ есть комплексный корень. $\square$

Следующие теоремы являются следствиями основной теоремы алгебры.

Теорема 102 (о разложении на линейные множители). *Всякий многочлен $f(x) \in \mathbb{C}[x]$, $\deg f(x) = n \geq 1$, над полем комплексных чисел раскладывается в произведение n линейных множителей.*

Доказательство. Индукция по n . При $n = 1$ многочлен является линейным. Предположим, что утверждение уже доказано для многочленов степени n , и пусть $f(x)$ — многочлен степени $n + 1$. Тогда

$f(x)$ имеет некоторый корень $\alpha_1 \in \mathbb{C}$, и по теореме Безу $f(x)$ представляется в виде $f(x) = (x - \alpha_1)f_1(x)$. Но многочлен $f_1(x)$ имеет степень n , и по предположению индукции раскладывается в произведение n линейных множителей. Но тогда $f(x)$ является произведением $n + 1$ линейного множителя. $\square$

Теорема 103 (о числе корней). *Всякий многочлен степени $n \geq 1$ с комплексными коэффициентами имеет n корней, если считать каждый корень столько раз, какова его кратность.*

Доказательство. Как мы только что доказали, многочлен степени $n \geq 1$ раскладывается в произведение n линейных множителей: $f(x) = a_0(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n)$. Ясно, что $\alpha_1, \dots, \alpha_n$ — это корни многочлена $f(x)$.

Объединяя равные сомножители в степени, $f(x)$ можно представить в виде

$$f(x) = a_0(x - \alpha_1)^{k_1}(x - \alpha_2)^{k_2} \dots (x - \alpha_s)^{k_s},$$

где корни $\alpha_1, \dots, \alpha_s$ уже все различны, а показатели $k_1, \dots, k_s$ — это кратности этих корней.

Поскольку степени многочленов в левой и правой частях этого равенства одинаковы, то $n = k_1 + k_2 + \dots + k_s$. $\square$

Упражнение 112. Многочлен $f(x)$ делится на многочлен $g(x)$ тогда и только тогда, когда всякий корень $f(x)$ является корнем $g(x)$ и кратность его в $g(x)$ не больше кратности в $f(x)$.

Указание. Используйте разложение многочленов $f(x)$ и $g(x)$ на линейные множители.

Теорема 104 (Виет). *Пусть*

$$f(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n, \quad a_0 \neq 0,$$

— многочлен с комплексными коэффициентами. Тогда для любого $k = 1, \dots, n$ сумма всевозможных произведений корней многочлена $f(x)$, состоящих из k сомножителей, равна $(-1)^k a_k / a_0$. В частности, сумма всех корней многочлена $f(x)$ равна $-a_1 / a_0$, сумма попарных произведений равна a_2 / a_0 , произведение всех корней равно $(-1)^n a_n / a_0$.

Доказательство. Представим $f(x)$ в виде:

$$f(x) = a_0(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n).$$

Тогда после раскрытия скобок в правой части имеем:

$$\begin{aligned} a_0x^n + a_1x^{n-1} + \dots + a_n &= \\ &= a_0x^n - a_0(\alpha_1 + \dots + \alpha_n)x^{n-1} + \dots + (-1)^n a_0\alpha_1\alpha_2 \dots \alpha_n. \end{aligned}$$

Если два многочлена равны, то равны их коэффициенты. Поэтому

$$-a_0(\alpha_1 + \dots + \alpha_n) = a_1, \dots, (-1)^n a_0\alpha_1 \dots \alpha_n = a_n. \quad \square$$

Теорема 105 (о разложении действительных многочленов). *Всякий многочлен степени $n \geq 1$ с действительными коэффициентами раскладывается в произведение линейных двучленов и квадратных трехчленов с отрицательными дискриминантами, имеющими действительные коэффициенты.*

Доказательство. Индукция по n . Для многочленов степени 1 и 2 утверждение верно. Предположим, что оно справедливо для любых многочленов степени, не большей n , и пусть $f(x)$ имеет степень $n+1$.

Многочлен $f(x)$ имеет комплексный корень α . По теореме Безу

$$f(x) = (x - \alpha)g(x), \quad (16)$$

и если число α действительное, то $g(x)$ — многочлен с действительными коэффициентами. Тогда по предположению индукции $g(x)$ раскладывается в произведение требуемого вида. Но тогда в силу (16) такое разложение существует и для многочлена $f(x)$.

Пусть теперь α — число не действительное, т. е. $\bar{\alpha} \neq \alpha$. По следствию из теоремы 93 число $\bar{\alpha}$ также является корнем многочлена $f(x)$. Тогда из (16) при $x = \bar{\alpha}$ получаем, что $f(\bar{\alpha}) = (\bar{\alpha} - \alpha)g(\bar{\alpha})$, и, следовательно, $g(\bar{\alpha}) = 0$. Снова применяя теорему Безу, имеем $g(x) = (x - \bar{\alpha})h(x)$, а тогда из (16) следует, что

$$f(x) = (x - \alpha)(x - \bar{\alpha})h(x) = (x^2 - (\alpha + \bar{\alpha})x + \alpha\bar{\alpha})h(x). \quad (17)$$

Так как $\alpha + \bar{\alpha}$ и $\alpha\bar{\alpha}$ — числа действительные, то трехчлен $x^2 - (\alpha + \bar{\alpha})x + \alpha\bar{\alpha}$ имеет действительные коэффициенты (и, очевидно, отрицательный дискриминант), значит, и многочлен $h(x)$ имеет действительные коэффициенты как частное двух многочленов с действительными коэффициентами.

Но многочлен $h(x)$ имеет степень меньше n , так что к нему применимо предположение индукции. После этого требуемое утверждение для многочлена $f(x)$ вытекает из равенства (17). $\square$

Приведем примеры применения доказанных теорем при решении задач.

Упражнение 113.

1. Докажите, что при любых натуральных p и q число $(p+1)^{2q+1} + p^{q+2}$ делится на $p^2 + p + 1$.

Решение. Рассмотрим многочлен $f(x) = (x+1)^{2q+1} + x^{q+2}$ и покажем, что он делится на квадратный трехчлен $x^2 + x + 1$. Этот трехчлен имеет два различных корня α и β и поэтому в силу доказанного выше следствия достаточно показать, что числа α и β являются корнями $f(x)$.

Заметим, что число α по определению таково, что $\alpha^2 = -\alpha - 1$, и, с другой стороны, $\alpha^2 + \alpha + 1 = \frac{\alpha^3 - 1}{\alpha - 1}$, так что $\alpha^3 = 1$. Поэтому

$$\begin{aligned} f(\alpha) &= (\alpha+1)^{2q+1} + \alpha^{q+2} = (-\alpha^2)^{2q+1} + \alpha^{q+2} = -(\alpha^2)^{2q+1} + \alpha^{q+2} = \\ &= -\alpha^{4q+2} + \alpha^{q+2} = \alpha^{q+2}(1 - \alpha^{3q}) = 0. \end{aligned}$$

Аналогично показывается, что $f(\beta) = 0$, так что $f(x)$ действительно делится на $x^2 + x + 1$. Способ деления углом показывает при этом, что частное $g(x)$ имеет целые коэффициенты, значит, выполняется равенство $f(p) = (p^2 + p + 1)g(p)$, в котором $g(p)$ — целое число.

2. При каких $n \in \mathbb{Z}$ число $n^{44} + n + 1$ простое?

Решение. При $n = 0$ и $n = -1$ это число равно 1 и простым не является, при $n = 1$ оно равно 3.

Докажем, что при всех остальных n число будет составным.

Рассмотрим многочлен $f(x) = x^{44} + x + 1$ и докажем, что он делится на квадратный трехчлен $x^2 + x + 1$. Пусть α и β — корни квадратного трехчлена. Тогда

$$f(\alpha) = \alpha^{44} + \alpha + 1 = \alpha^2 + \alpha + 1 = 0,$$

аналогично $f(\beta) = 0$. В силу доказанной выше теоремы

$$x^{44} + x + 1 = (x^2 + x + 1) \cdot P(x),$$

где $P(x)$ — многочлен с целыми коэффициентами.

Так как при $n \in \mathbb{Z}$, $n \neq 0$, $n \neq 1$, $n \neq -1$ очевидно $n^{44} + n + 1 > n^2 + n + 1$, то $n^2 + n + 1$ — нетривиальный делитель.

3. Разложить на множители многочлены $x^5 + x + 1$ и $x^{10} + x^5 + 1$.

Решение. Заметим, что если α является корнем квадратного трехчлена $x^2 + x + 1$, то $\alpha^3 = 1$, и тогда

$$\alpha^5 + \alpha + 1 = \alpha^2 + \alpha + 1 = 0, \quad \alpha^{10} + \alpha^5 + 1 = \alpha + \alpha^5 + 1 = 0.$$

Следовательно, многочлены $x^5 + x + 1$ и $x^{10} + x^5 + 1$ делятся на $x^2 + x + 1$. Частные от деления найдите самостоятельно.

Задачи и упражнения к § 4.11

1. Решите уравнения: а) $x^6 + 27 = 0$; б) $x^{2n} - 2x^n + 2 = 0$.
2. Постройте многочлен из $\mathbb{R}[x]$ наименьшей степени с трехкратным корнем $2 + 3i$.
3. Составьте уравнение 6-й степени с корнями $\alpha, 1/\alpha, 1 - \alpha, 1 - 1/\alpha, 1/(1 - \alpha), 1/(1 - 1/\alpha)$.
4. Разложите на множители над полями действительных и комплексных чисел многочлены: а) $x^n - 1$; б) $x^n + 1$; в) $x^{2n} + x^n + 1$.
5. Решите уравнения:
 - а) $(x^2 - x + 1)^3 - a(x^2 - x)^2$ при $a = (\alpha^2 - \alpha + 1)^3/(\alpha^2 - \alpha)^2$;
 - б) $(x + 1)^n - (x - 1)^n = 0$;
 - в) $(x + i)^n - (x - i)^n = 0$.
6. Докажите, что если $|a| = 1$, то все корни уравнения $(ix + 1)^n = a(1 - ix)^n$ действительны.
7. Докажите, что многочлен $x^{3n} + x^{3m+1} + x^{3k+2}$ делится на $1 + x + x^2$.
8. При каких значениях m многочлен $(x + 1)^m + x^m + 1$ делится на $1 + x + x^2$?
9. Если $F(x) = f_1(x^3) + x f_2(x^3)$ делится на $1 + x + x^2$, то f_i делится на $x - 1$.
- 10*. Если многочлен $f(x) \in \mathbb{R}[x]$ и не принимает при $x \in \mathbb{R}$ отрицательных значений, то он представим в виде суммы квадратов двух многочленов из $\mathbb{R}[x]$.
- 11*. Пусть $M_k(x_k, y_k)$ — точки на плоскости, $y_k > 0$ при $k \leq m$ и $y_k < 0$ при $k > m$. На оси абсцисс расположены точки A_l , $1 \leq l \leq n + 1$, так, что для любого l

$$\sum_{k=1}^m \angle M_k A_l \infty = \sum_{k=m+1}^n \angle M_k A_l \infty,$$

где $\angle M_k A_l \infty$ — угол между вектором $A_l M_k$ и положительным направлением оси абсцисс. Докажите, что множество всех точек M_k симметрично относительно оси абсцисс.

12. Если $a_1, \dots, a_n$ — вершины правильного n -угольника с центром в a , то для любого многочлена $f(x) \in \mathbb{C}[x]$ степени, меньшей n ,

$$f(a_1) + \dots + f(a_n) = n f(a).$$

13. Дробно-рациональная функция называется: *правильной*, если степень числителя меньше степени знаменателя; *примарной* над данным полем, если знаменатель является степенью неприводимого над данным полем многочлена; *простейшей*, если она примарна и степень числителя меньше степени этого многочлена. Докажите, что сумма и произведение

правильных дробей — правильные, и любая дробь есть сумма многочлена и правильной дроби, причем это представление — однозначно.

14*. Правильная дробь разлагается в сумму примарных дробей с взаимно простыми знаменателями, причем это представление однозначно.

15*. Примарная дробь разлагается в сумму простейших дробей, причем это представление однозначно.

16*. Разложите над полями $\mathbb{C}$ и $\mathbb{R}$ дробь $1/(x^{2n} + 1)$ на простейшие.

§ 4.12. Как решать уравнения на экзаменах

В этом параграфе на основе изложенного материала дадим сводку основных приемов решения алгебраических и сводящихся к ним уравнений.

Уравнения первой степени, надеемся, читатель умеет решать. Квадратные уравнения обсуждались в § 1.5. Трудности возникают только с уравнениями высоких степеней.

Дадим несколько советов, отсылая за подробностями к соответствующим параграфам книги.

Вначале надо проверить, не имеет ли уравнение специальный вид, для которого есть свой метод решения. Например, не является ли оно биквадратным, или уравнением вида $af(x)^2 + bf(x) + c = 0$, сводящимся к квадратному какой-нибудь заменой переменных $y = f(x)$. После этого придется решать одно или два уравнения вдвое меньшей степени. Подобные приемы решения называются понижением степени уравнения.

Легко понижается степень четных или нечетных уравнений. Если многочлен $p(x)$ не является ни тем, ни другим, но удовлетворяет равенству $p(x) = p(a - x)$ при некоторой константе a , то у уравнения $p(x) = 0$ можно понизить степень с помощью замены $y = x(a - x)$.

Упражнение 114. Докажите это и решите уравнение

$$x^4 - 2x^3 - 2x^2 + 3x + 2 = 0.$$

В § 3.9 показано, как понижать степень у возвратных уравнений с помощью замены $y = x + 1/x$.

Упражнение 115. Решите уравнение

$$x^6 - 10x^4 - 12x^3 - 10x^2 + 1 = 0.$$

Если уравнение имеет вид $f(f(x)) = x$ или подобный, то можно его решить приемами, указанными в § 3.7, посвященном итерациям и приложенным методам.

Если же ни один из указанных приемов не работает, то пытаемся понизить степень уравнения, разложив его на множители. Если очевидным

образом оно не разлагается, то приступаем к систематическому поиску разложения. Начать лучше всего с наиболее простых и знакомых вам приемов. Например, с простого поиска рациональных корней методом Гаусса, описанным в задаче 11 из §3.2. Он применим только к уравнениям с рациональными коэффициентами, причем предварительно их коэффициенты надо сделать целыми путем умножения на подходящее целое число.

Упражнение 116. 1. Решите уравнение Бхаскары *

$$x^4 - 2x^2 - 400x - 9999 = 0.$$

2. Решите уравнение Бомбелли ** $x^3 = 15x + 4$.

Если рациональных корней найти не удалось, то надо искать разложение на множители более высоких степеней. В §3.8 было доказано, что если коэффициенты многочлена целые, то его разложение можно искать среди таких же многочленов, причем оно определено фактически однозначно. Однако многочлен может оказаться и неприводимым. Чтобы зря не тратить время на поиск его разложения, может быть полезно применить один из признаков неприводимости из §3.8. Но это совет для пессимистов.

Для уравнений четвертой степени поиск разложения можно провести *методом неопределенных коэффициентов*. Этот метод, предложенный Декартом, заключается в том, что в искомом разложении неизвестные коэффициенты обозначаются четырьмя буквами, вычисляются буквенные выражения коэффициентов произведения и приравниваются к известным коэффициентам уравнения, после чего полученная система решается подбором целых значений коэффициентов. Указанный прием не является, конечно, алгоритмом, но иногда ускоряет поиск разложения. Однако его применение для уравнений степени выше четвертой, как правило, затруднительно.

Упражнение 117. Решите уравнение Луки Пачоли ***

$$x^4 + 2x^3 + 3x^2 + 2x - 81600 = 0.$$

Гарантированно найти разложение можно, применяя алгоритм Кронекера (см. §3.8), хотя это очень трудоемкая процедура.

* Бхаскара Ачарья (1114–1178) — индийский математик и астроном.

** Р. Бомбелли (Raffaele Bombelli, 1530–1572) — итальянский математик и инженер. Первым открыл комплексные числа.

*** Л. Пачоли (Luca Pacioli, 1445–1517) — итальянский математик. Написал трактат о золотом сечении. Друг Леонардо да Винчи.

Упражнение 118. Решите методом Кронекера уравнение

$$x^5 + x + 1 = 0.$$

На практике уравнения с кратными корнями встречаются редко, а в задачах и на экзаменах — довольно часто. Если есть подозрение о наличии кратных корней, иногда лучше сразу их отделить одним из методов бесквадратной факторизации (см. § 3.12).

Упражнение 119. Решите уравнение

$$x^6 + x^5 - 3x^3 - 4x^2 - 3x - 1 = 0.$$

Методы эти трудоемки, так как при применении алгоритма Евклида быстро растут коэффициенты (борьба с этим явлением, которое встречается и в других ситуациях, — одна из проблем компьютерной алгебры). Но зато они применимы не только к многочленам с целыми коэффициентами.

Упражнение 120. Решите уравнение $x^3 + 6x = (3x^2 + 2)\sqrt{2}$.

Впрочем, это уравнение можно решить, просто угадав корень.

Угадывание корней — вполне законный прием. Для некоторых неалгебраических (трансцендентных) уравнений это единственное, что остается.

Упражнение 121. Угадайте корень уравнения $x^{x^4} = 4$.

После того как корень угадан, можно попытаться доказать, что других корней нет. Обычно для этого используют технику неравенств, в частности соображения монотонности.

Упражнение 122. Докажите, что уравнение $x^{x^4} = 4$ имеет единственный корень.

Для алгебраических уравнений развиты различные методы для определения числа корней в данных интервалах, для их оценки и для так называемого разделения корней, служащего первым этапом перед их приближенным вычислением. Мы не собираемся излагать здесь эти методы, а ограничимся некоторым представлением о них, которое можно получить в § 4.1 и в задачах из § 4.18. Заметим, что методы приближенного вычисления корней можно использовать и для их угадывания, особенно если под рукой есть калькулятор.

А когда же надо применять формулы для решения уравнений третьей и четвертой степени? Только тогда, когда упомянутые выше элементарные приемы не дали результата. Например, если вы доказали, что кубическое уравнение с рациональными коэффициентами не имеет рациональных корней, то остается только применить формулу Кардано, а в неприводимом случае сделать тригонометрическую подстановку

и получить тригонометрическое решение. Заметим, что если уравнение не имеет канонического вида $x^3 + px + q = 0$, то иногда более красивые тригонометрические решения получаются, если применить какой-нибудь искусственный прием, как, например, в задаче 10 из § 4.2.

В § 4.19 будет доказано, что если кубическое уравнение с рациональными коэффициентами не имеет рациональных корней, то его корни нельзя выразить только через квадратные радикалы, т. е. решить «школьным» методом.

Если уравнение четвертой степени с рациональными коэффициентами не удалось решить элементарно, то можно, например, применить метод Феррари, найти кубическую резольвенту, потом какой-нибудь один ее корень и разложить уравнение на квадратные множители. Если резольвента имеет рациональный корень, то его проще всего искать угадыванием (или методом поиска рациональных корней). Тогда полученное разложение будет иметь целые коэффициенты, и все корни выражаются через квадратные радикалы. Найдя решение, можно его представить как полученное «школьным» методом, например, угадыванием разложения на множители.

Если же кубическая резольвента не имеет рациональных корней, то можно доказать, что корни исходного уравнения четвертой степени нельзя выразить только через квадратные радикалы (см. § 4.19), а значит, и решить «школьным» методом.

Если мы хотим в этом случае написать явные формулы в радикалах, лучше использовать не метод Феррари, а метод Лагранжа или Эйлера.

Рассмотрим кратко приемы решения неалгебраических уравнений. Простейшие из них — это рациональные уравнения, т. е. уравнения, в обеих частях которых стоят рациональные дроби. Рациональная дробь — это частное двух многочленов. Мы не излагали строгого построения рациональных дробей, полагая, что сведений из средних классов школы об этом достаточно. Рациональные уравнения, как известно, легко сводятся к алгебраическим, если выполнить все операции над дробями в ненулевой части уравнения. Нужна только некоторая внимательность, так как, приравнявая к нулю числитель дроби в ненулевой части уравнения, мы получаем алгебраическое уравнение, не равносильное исходному, потому что оно может иметь корни, не входящие в область определения исходного уравнения. Такие корни называются посторонними и их надо отбрасывать.

Заметим, однако, что не всегда надо торопиться приводить рациональное уравнение к алгебраическому виду. Если решение полученного уравнения вызывает трудности и требует искусственных приемов, то имеет смысл вернуться к исходному уравнению, так как для него иногда легче

увидеть искомый искусственный прием. Например, уравнение

$$1/x^2 + 2/x + 2x + x^2 = 5$$

можно свести к алгебраическому возвратному, но стоит ли это делать, когда для него замена переменной $y = x + 1/x$ видна еще лучше.

Упражнение 123. Решите это уравнение.

А в следующем примере легко угадываются корни.

Упражнение 124. Решите уравнение

$$\frac{x-a}{b} + \frac{x-b}{a} = \frac{b}{x-a} + \frac{a}{x-b}.$$

Не всегда надо раскрывать скобки даже в алгебраическом уравнении. В следующем уравнении замену $y = x/12$ удобно делать, их не раскрывая.

Упражнение 125. Решите уравнение

$$(12x - 1)(6x - 1)(4x - 1)(3x - 1) = 5.$$

Более сложными для решения являются *иррациональные* уравнения. По существу это тоже алгебраические уравнения, но содержащие радикалы. Их можно рассматривать и над полем комплексных чисел, но тогда они становятся многозначными и нужны специальные договоренности о том, что понимается под их решениями. Обычно такие уравнения рассматривают только в поле действительных чисел, поэтому решение их приходится начинать с определения области допустимых значений уравнения. Для этого решается система неравенств, которая выражает неотрицательность всех выражений под радикалами четного порядка. Уже эта система может быть сама иррациональной и ее решение иногда бывает затруднительным. Поэтому часто ее вообще не решают, а стараются выполнять при решении уравнения только эквивалентные преобразования, добавляя в случае необходимости соответствующие неравенства к преобразованному уравнению. Преобразования, как правило, представляют из себя возведение обеих частей уравнения в одну и ту же степень с целью избавления от некоторых радикалов. В сложных уравнениях приходится делать несколько таких преобразований до полного уничтожения радикалов.

Полная теория решения иррациональных уравнений достаточно сложна и имеет мало реальных применений, поэтому обычно нигде не излагается. В пособиях для абитуриентов рассматривают наиболее используемые приемы их решения. Мы тоже ограничимся несколькими замечаниями.

Как правило, перед выполнением такого преобразования в одной части уравнения оставляют один радикал, а остальные собирают в другой части (этот прием называется уединением радикала). Заметим, что иногда

после такого преобразования число радикалов не уменьшается, а возрастает. Например, если во второй части стоит сумма четырех квадратных радикалов, то после возведения в квадрат их станет шесть. В таких довольно редких случаях иногда лучше распределить радикалы между частями уравнения более равномерно, например, в рассматриваемом случае два радикала с одной стороны, а три с другой.

Но и это не всегда помогает. Например, рассмотрим уравнение вида

$$\sqrt{a_1} + \sqrt{a_2} + \sqrt{a_3} = \sqrt{a_4} + \sqrt{a_5} + \sqrt{a_6}.$$

Здесь как ни распределяй радикалы, после возведения в квадрат их станет еще больше. Чтобы получить представление об общем методе сведения иррациональных уравнений к алгебраическим, покажем, как избавиться от радикалов в уравнении вида

$$\sqrt{a_1} + \sqrt{a_2} + \sqrt{a_3} = b,$$

не перенося радикалы в правую сторону. Для этого заметим, что если раскрыть скобки в произведении всех восьми выражений вида

$$X - \sigma_1\sqrt{a_1} - \sigma_2\sqrt{a_2} - \sigma_3\sqrt{a_3}, \quad \sigma_1 = \pm 1, \quad \sigma_2 = \pm 1, \quad \sigma_3 = \pm 1,$$

то получится многочлен от X восьмой степени, коэффициенты которого будут многочленами от переменных a_i и не будут содержать радикалов. В этом можно убедиться непосредственно, разбивая сомножители на пары вида $(A + \sqrt{a_3})$ и $(A - \sqrt{a_3})$ и перемножая их по правилу разности квадратов. Таким образом избавляемся от $\sqrt{a_3}$, после чего получится 4 произведения (квадратные трехчлены от X), которые разбиваем на пары аналогичным образом, и т. д. Подставим вместо X в полученный многочлен выражение

$$b = \sqrt{a_4} + \sqrt{a_5} + \sqrt{a_6}$$

и раскроем скобки. Получится сумма восьми слагаемых вида

$$b_{\alpha_1, \alpha_2, \alpha_3} \sqrt{a_4^{\alpha_1} a_5^{\alpha_2} a_6^{\alpha_3}}, \quad \alpha_i = 0, 1, \quad i = 1, 2, 3,$$

где $b_{\alpha_1, \alpha_2, \alpha_3}$ являются многочленами от переменных a_i , $i = 1, \dots, 6$. Это утверждение становится очевидным, если заметить, что множество F всех сумм указанного вида замкнуто относительно сложения и умножения. Наше уравнение переписывается теперь как равенство нулю полученной суммы. Перепишем его в виде

$$-b_{0,0,0} = \sum_{(\alpha_1, \alpha_2, \alpha_3) \neq (0,0,0)} b_{\alpha_1, \alpha_2, \alpha_3} \sqrt{a_4^{\alpha_1} a_5^{\alpha_2} a_6^{\alpha_3}} = f,$$

где $b_{0,0,0} \neq 0$. Вычислим степени $f^2, \dots, f^8$ и заметим, что все они принадлежат множеству F . Принимая произведения

$$\sqrt{a_4^{\alpha_1} a_5^{\alpha_2} a_6^{\alpha_3}}, \quad \alpha_i = 0, 1, \quad i = 1, 2, 3,$$

за новые неизвестные $y_{\alpha_1, \alpha_2, \alpha_3}$, $\alpha_i = 0, 1$, $i = 1, 2, 3$, можно, последовательно исключая переменные из полученной линейной системы*, выразить $1 = y_{0,0,0}$ в виде

$$c_1 f + \dots + c_8 f^8,$$

где c_i — дробно-рациональные выражения от переменных a_i , $i = 1, \dots, 6$. Заменяя f на многочлен $-b_{0,0,0}$ от тех же переменных, сводим полученное рациональное уравнение к алгебраическому уравнению относительно переменных a_i , $i = 1, \dots, 6$. Подставляя в него вместо a_i заданные выражения из исходного уравнения, получаем уравнение, которое является его следствием, но не содержит указанных шести радикалов.

Разумеется, полученное уравнение (или то уравнение, к которому его придется далее сводить) будет содержать массу посторонних корней, которые придется отбрасывать после проверки.

Сведение иррационального уравнения к алгебраической системе уравнений и неравенств даже в несложных на вид уравнениях может быть достаточно громоздким. В этих случаях естественно попробовать поискать какой-нибудь искусственный прием для решения, вроде тех, которые применялись к алгебраическим уравнениям. Например, угадать корень и воспользоваться монотонностью или каким-нибудь подходящим неравенством либо сделать замену переменных, иногда даже две.

Упражнение 126. Решите уравнение $\sqrt[3]{6x+28} - \sqrt[3]{6x-28} = 2$.

Упражнение 127. Решите уравнение $\sqrt{x-1/x} + \sqrt{1-1/x} = x$.

Уравнения с модулями тоже входят в класс иррациональных уравнений, так как каждый модуль можно заменить на радикал по формуле $|x| = \sqrt{x^2}$. Используя этот прием, можно избавиться от модулей с помощью возведений в квадрат. Иногда это помогает, но чаще проще избавиться от модулей простым перебором случаев.

Некоторые приемы позволяют уменьшить количество рассматриваемых вариантов. Например, при решении уравнений вида

$$|x - a_1| + \dots + |x - a_n| = b$$

формально надо рассмотреть при раскрытии модулей 2^n вариантов, а на самом деле достаточно заметить, что на каждом из отрезков

* Как это делать, описано в следующем параграфе.

$[a_i, a_{i+1}]$ рассматриваемая функция линейна, и чтобы, например, нарисовать ее график, достаточно вычислить ее значения в точках a_i , что требует порядка n^2 операций сложения и вычитания.

Следующий класс уравнений называется классом *трансцендентных* уравнений и включает все остальные уравнения. В нем выделяют подклассы логарифмических, показательных и тригонометрических уравнений, но часто встречаются также и смешанные уравнения, в которых участвуют все элементарные функции, в том числе и радикалы, и обратные тригонометрические, а иногда даже и знаки целой части. Понятно, что общей теории таких уравнений не существует, однако приближенно их корни можно вычислять, например методом вилки или методом Ньютона.

Для их решения применяются самые разнообразные искусственные приемы (трюки), например, угадывание корней и пр.

Упражнение 128. Решите уравнение $16^x = \log_{\frac{1}{16}} x$.

Упражнение 129. Решите уравнение $3^x + 4^x = 5^x$.

Но на экзаменах обычно предлагаются уравнения, которые легко (или не очень) сводятся к алгебраическим уравнениям, как правило, квадратным.

Как это делать для некоторых классов тригонометрических уравнений, будет ясно после прочтения §4.17. Однако для решения тригонометрических уравнений есть масса своих собственных приемов, в основном связанных с разложением на множители, которые позволяют достичь цели быстрее, чем методы из §4.17. Здесь мы не будем их излагать.

Задачи и упражнения к § 4.12

Решите уравнения

1. (Харриот.) $x^3 - 3x - 52 = 0$.
2. (Стевин.) $Px^3 - 6x - 40 = 0$.
3. (Жирар.) (i) $x^3 - 13x - 12 = 0$; (ii) $x^3 - 4x + 3 = 0$.
4. (Декарт.) (i) $x^3 - 8x^2 - x + 8 = 0$; (ii) $x^3 - 9x^2 + 26x - 24 = 0$;
- (iii) $x^4 - 4x^3 - 19x^2 + 106x - 120 = 0$.
5. (Кардано.) $x^4 + 2x^3 + 2x + 1 = 13x^2$.
6. (Монферрье.) $x^6 + 3x^5 + 2x^4 - 2x^2 - 3x - 1 = 0$.
7. Докажите, что уравнение $\frac{x^{2n}}{(2n)!} + \dots + \frac{x^3}{3!} + \frac{x^2}{2!} + x + 1 = 0$ не имеет действительных корней.

8. Решите уравнение

$$\frac{(-1)^n x(x-1) \dots (x-n+1)}{n!} + \dots + \frac{x(x+1)}{2!} - \frac{x}{1!} + 1 = 0.$$

§ 4.13. Системы уравнений

Системы уравнений, встречавшиеся ранее, были в основном симметрическими. Алгоритм их решения был изложен в § 3.10 о симметрических многочленах.

Заметим, однако, что не следует торопиться сводить систему к теореме Виета, как рекомендовано в этом параграфе. Иногда проще угадать решение, а потом доказать, что других решений нет.

Упражнение 130. Решите систему

$$\begin{cases} x + y + z + w = 10; \\ x^2 + y^2 + z^2 + w^2 = 30; \\ x^3 + y^3 + z^3 + w^3 = 100; \\ xyzw = 24. \end{cases}$$

После того как вы угадали одно решение, можно получить и остальные решения, выполнив все 24 перестановки его компонент. Отсутствие других решений вытекает, например, из теоремы Безу о том, что система алгебраических уравнений имеет число решений, не большее произведения степеней ее уравнений, если, конечно, она не является неопределенной и имеющей поэтому бесконечно много решений. Но доказательство этой теоремы сложно, и мы не будем его приводить. Поэтому лучше представим, что мы свели все-таки систему к системе Виета, и заметим, что система Виета n -го порядка имеет не более $n!$ решений, причем имеет ровно $n!$ решений, если соответствующее уравнение не имеет кратных корней. Впрочем, система может не иметь решений, если не все корни уравнения принадлежат рассматриваемому полю.

При решении несимметричных систем часто применяют разнообразные искусственные приемы, например, итерации, как в § 3.7.

Упражнение 131. Решите систему из § 3.7

$$\begin{cases} y = x^2 - 1; \\ z = y^2 - 1; \\ x = z^2 - 1. \end{cases}$$

Используют идеи, заимствованные из комплексных чисел, как в § 4.3.

Упражнение 132. Решите систему из § 4.3

$$\begin{cases} x - \frac{x - 3y}{x^2 + y^2} = 2; \\ y + \frac{3x + y}{x^2 + y^2} = 3. \end{cases}$$

Применяют неравенства, как в следующей системе.

Упражнение 133. Решите систему

$$\begin{cases} x^{2002} + y^{2002} = 1; \\ x^2 + y^2 = 1. \end{cases}$$

Хотя она и симметричная, применять для ее решения общий метод решения таких систем неразумно. Неравенства помогают решать и системы, в которых число уравнений меньше числа неизвестных, например, следующую, которую, правда, можно решить и как симметрическую систему.

Упражнение 134. Решите систему

$$\begin{cases} xyz = 8; \\ x^2 + y^2 + z^2 = 12. \end{cases}$$

Иногда помогает разложение на множители.

Упражнение 135. Решите систему

$$\begin{cases} 2x^2 + 3xy - 2y^2 - 6x + 3y = 0; \\ 3x^2 + 7xy + 2y^2 - 7x + y - 6 = 0. \end{cases}$$

Но наиболее распространенные приемы — это всевозможные замены переменных. Например, этот прием хорошо работает для симметрических систем.

Простейший его вариант — это выражение из одного уравнения одной неизвестной через другие и подстановка этого выражения в оставшиеся уравнения, после чего получается система с меньшим числом неизвестных или даже одно уравнение. Для его применения надо найти одно из уравнений системы, разрешимое относительно одной из неизвестных. Теоретически это возможно, если эта неизвестная входит в уравнение в степени не выше четвертой, однако если полученное выражение будет содержать радикалы, вряд ли оно вам поможет. Но попробовать всегда имеет смысл, так как радикалы могут и не появиться. Например, если одно из уравнений однородное с двумя неизвестными и с нулевой правой частью, то отношение неизвестных можно найти, решая уравнение с постоянными коэффициентами.

Упражнение 136. Решите систему

$$\begin{cases} x^4 + kx^3y - 6x^2y^2 - kxy^3 + y^4 = 0; \\ x^2 + y^2 = 1. \end{cases}$$

Наличие в системе параметра не должно вас смущать — от него ответ зависеть не будет, хотя в общем случае зависит, и еще как.

Самый простой, но в тоже время и самый важный класс систем уравнений — это системы первой степени, или *линейные* системы. Большая

часть систем уравнений, которые приходится решать во нематематических приложениях, как раз и составляют линейные системы. Их теория разработана лучше всего и лежит в основе важного раздела алгебры — так называемой *линейной алгебры*. Изучение элементов линейной алгебры периодически включалось в курсы алгебры в ФМШ МГУ, но в последнее время это делалось очень редко, в основном по причине нежелания дублировать университетский курс. Мы здесь поэтому ограничимся только начальными сведениями о линейных системах.

Прием, которым они решаются, — все то же исключение неизвестных, и делается оно для них особенно просто. В первом уравнении выражается первая же неизвестная через остальные (как говорят в линейной алгебре, в виде *линейной комбинации* остальных неизвестных), ее выражение подставляется в остальные уравнения и получается линейная система с меньшим числом уравнений и неизвестных. К ней применяется тот же прием, пока не получится одно уравнение.

Здесь могут возникнуть три случая. В первом случае, наиболее часто встречающемся в системах, взятых из задачников, получается линейное уравнение с одной неизвестной, которое легко решается*.

Во втором случае получается уравнение с несколькими неизвестными. В этом случае говорят, что система *неопределенная*, так как она имеет бесконечно много решений. Чтобы их все найти, надо принять все неизвестные из последнего уравнения, кроме одного, за параметры и выразить через них (в виде линейной комбинации) все оставшиеся неизвестные. Если число параметров равно k , то говорят, что система имеет *k -мерное пространство решений*.

В третьем случае получается не уравнение, а просто неверное равенство, которое означает, что система не имеет решения (система *несовместна*).

Решать линейные системы научились давно, но этот метод по традиции называют с именем Гаусса.

Упражнение 137. Решите систему Ямвлиха**

$$\begin{cases} x + y = 2(z + u); \\ x + z = 3(y + u); \\ x + u = 4(y + z). \end{cases}$$

* Впрочем, легко только для того, кто знает, что такое дроби. Древние египтяне, которые, видимо, первыми научились решать такие уравнения, построили для этого довольно экзотическую, с современной точки зрения, теорию рациональных дробей.

** Ямвлих — древнегреческий математик, философ и мистик, написавший книгу об Элевсинских мистериях.

Элементарные преобразования можно применять не только к линейным системам. Можно для произвольных систем в определении элементарных преобразований разрешить умножение не на константу, а на произвольное выражение.

Упражнение 140. Решите систему

$$\begin{cases} x - y = x^2 y^2; \\ y^3 + x^4 y + y^4 x = 0. \end{cases}$$

В терминах элементарных преобразований метод Гаусса можно представить следующим образом. Выполняется последовательность элементарных преобразований, которая приводит систему к треугольной или трапециевидной.

Система с квадратной матрицей называется *треугольной*, если в ее матрице $m \times m$ все элементы $a_{i,j}$, $i > j$, расположенные ниже диагонали, равны нулю, но $a_{1,1} \dots a_{m,m} \neq 0$.

Система называется *трапециевидной*, если в ее матрице $a_{1,1} \dots a_{k,k} \neq 0$, в строках $(k+1)$ -й и ниже (если они есть) стоят только нули и ниже диагонали — тоже нули.

Упражнение 141. Если система треугольная, то она имеет единственное решение, которое можно найти за $n(n-1)$ операций.

Упражнение 142. Если система трапециевидная, то она либо не имеет решений, если нулевой строке матрицы системы соответствует ненулевой коэффициент в правой части соответствующего уравнения, либо в противном случае имеет $(n-k)$ -мерное пространство решений.

Упражнение 143. Сложность алгоритма Гаусса оценивается сверху как Cn^3 .

В применении алгоритма Гаусса к большим системам на компьютерах возникает много проблем, связанных как с возникновением слишком больших коэффициентов (*переполнение*), так и с делением на слишком малые числа (*машинный ноль*). В результате исследований этих вопросов появились много разных компьютерных алгоритмов для решения линейных систем, изложению которых посвящены целые книги. Мы не будем здесь касаться этих интересных вопросов.

Решение теоретических вопросов, связанных с линейными системами, было завершено в XIX в. В результате появились теория матриц и теория определителей, которые, как выяснилось со временем, играют важную роль в математике и без прямой связи с линейными системами. Мы не можем здесь излагать эти теории, укажем лишь кратко геометрическую интерпретацию линейных систем.

Каждое из уравнений системы второго порядка

$$\begin{cases} a_{1,1}x_1 + a_{1,2}x_2 = b_1; \\ a_{2,1}x_1 + a_{2,2}x_2 = b_2 \end{cases}$$

можно представить как прямую линию на плоскости с уравнением

$$a_{i,1}x_1 + a_{i,2}x_2 = b_i, \quad i = 1, 2.$$

Множество всех решений системы совпадает с пересечением этих прямых линий. Если линии параллельны и не совпадают, то система несовместна. Если они совпадают — а это означает, что их коэффициенты пропорциональны:

$$\frac{a_{1,1}}{a_{2,1}} = \frac{a_{1,2}}{a_{2,2}} = \frac{b_1}{b_2},$$

— то система неопределена и имеет одномерное пространство решений. Если прямые не параллельны, то система имеет единственное решение, которое соответствует точке пересечения этих прямых.

В случае линейной системы с тремя неизвестными уравнениям соответствуют плоскости в трехмерном пространстве. Если среди них есть параллельные и несовпадающие, то система несовместна. Если есть совпадающие, то соответствующие уравнения можно из системы удалить, не меняя множества ее решений. Пара непараллельных плоскостей пересекается по прямой линии. Если эта прямая параллельна остальным плоскостям, то система несовместна, а если она совпадает с пересечением остальных плоскостей, то пространство решений системы одномерно. Если все плоскости совпадают друг с другом, то пространство решений системы двумерно. В оставшемся случае пересечение трех плоскостей является одной точкой. Если больше уравнений нет, то система имеет одно решение, так же как и в случае, когда остальные плоскости тоже проходят через эту точку. В противном случае система несовместна.

Попытка дать геометрическую интерпретацию линейных систем n -го порядка привела к созданию геометрии n -мерного пространства, которой мы не будем здесь заниматься.

Для системы второго порядка

$$\begin{cases} a_{1,1}x_1 + a_{1,2}x_2 = b_1; \\ a_{2,1}x_1 + a_{2,2}x_2 = b_2 \end{cases}$$

нетрудно вывести и явные формулы для решений, именно

$$x_1 = \frac{b_1 a_{2,2} - b_2 a_{1,2}}{a_{1,1} a_{2,2} - a_{2,1} a_{1,2}}, \quad x_2 = \frac{b_1 a_{2,1} - b_2 a_{1,1}}{a_{1,1} a_{2,2} - a_{2,1} a_{1,2}},$$

если $a_{1,1}a_{2,2} - a_{2,1}a_{1,2} \neq 0$. Подобные формулы уже для систем третьего порядка громоздки, а далее становятся просто необозримыми. Поэтому Лейбниц ввел понятие определителя квадратной матрицы $n \times n$.

Определение 102. *Определителем (или детерминантом) матрицы A размера $n \times n$ с элементами $a_{i,j}$ называется сумма всех $n!$ произведений вида $a_{1,\pi(1)} \dots a_{n,\pi(n)}$, каждое из которых соответствует одной из $n!$ различных перестановок π и берется со знаком $\varepsilon(\pi)$, равным знаку этой перестановки. Сокращенно определитель матрицы обозначается $\det(A)$, а иногда и просто $|A|$.*

Формулы Крамера для решения системы уравнений с матрицей A и столбцом свободных членов b , которые мы не будем доказывать, имеют вид

$$x_i = \frac{\det(A_i)}{\det(A)},$$

где A_i — матрица, которая получается, если в матрице A заменить i -й столбец, состоящий из чисел $a_{1,i}, \dots, a_{n,i}$, на столбец, состоящий из чисел $b_1, \dots, b_n$.

Но чтобы читатель получил все же некоторое представление о теории определителей, предлагаем ему несколько упражнений.

Упражнение 144. Проверьте, что определитель меняет знак при перестановке любых двух строк или любых двух столбцов и не меняется при остальных элементарных преобразованиях его матрицы, выполненных как со строками, так и со столбцами.

Упражнение 145. Напишите явные формулы определителей второго и третьего порядков. Докажите формулы для решения линейных систем второго и третьего порядков.

Упражнение 146. Определитель треугольной матрицы равен произведению диагональных элементов. Определитель трапециевидной матрицы равен нулю.

Упражнение 147. Непосредственное вычисление определителя n -го порядка требует $n \cdot n! - 1$ умножений и сложений-вычитаний.

Поэтому явную формулу используют для вычислений только при $n \leq 3$ и иногда при $n = 4$. А вычисляют определители методом Гаусса, преобразовывая матрицу к треугольной (или трапециевидной).

Упражнение 148. Докажите, что определитель n -го порядка можно вычислить за Sn^3 арифметических операций в поле, над которым рассматривается матрица.

Формулы Крамера имеют поэтому только теоретическое значение, и при $n > 3$ для решения систем используется метод Гаусса без предварительного вычисления определителей.

Определитель можно геометрически интерпретировать как ориентированный объем параллелепипеда, натянутого на ее столбцы (или строки). Мы поясним это утверждение только в двумерном случае. При $n = 2$ определитель матрицы $\begin{vmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{vmatrix}$ равен площади параллелограмма, натянутого на вектора $(a_{1,1}a_{1,2})$, $(a_{2,1}a_{2,2})$, которая берется со знаком плюс, если первый вектор переходит во второй при повороте против часовой стрелки.

Для доказательства совпадения ориентированной площади и определителя можно проверить, что ориентированная площадь обладает теми же свойствами, что и определитель, указанными в предыдущих упражнениях. Остается только заметить, что определитель *единичной матрицы* (матрицы с единицами на главной диагонали a_{ii} и нулями вне ее) равен единице, так же как и соответствующая ориентированная площадь.

Хотя в основном линейная алгебра была создана в XIX в., ее развитие продолжается и сейчас. Например, немецкий математик Штрассен в 1967 году предложил алгоритм для решения линейных систем n -го порядка и соответствующих определителей со сложностью $Cn^{\log_2 7}$. Этот результат вызвал сенсацию, но, к сожалению, алгоритм Штрассена начинает превосходить алгоритм Гаусса только для матриц порядка нескольких сотен. В дальнейшем оценка Штрассена усилиями его самого и других математиков неоднократно улучшалась и доведена сейчас до оценки Cn^τ , где $\tau < 2,35$, однако гипотеза Штрассена о том, что можно получить оценку, в которой $\tau \rightarrow 2$, еще не доказана, а полученные новые алгоритмы превосходят алгоритм Штрассена только для матриц колоссальных размеров и не имеют практического значения.

Некоторые нелинейные системы легко сводятся к линейным. Приведем простейшие примеры, в которых сведение осуществляется логарифмированием. Разумеется, можно логарифмирования не делать, а повторить на мультипликативном языке то, что делается с соответствующей линейной системой на аддитивном.

Упражнение 149. Решите систему $\begin{cases} xy = 5; \\ yz = 6; \\ xz = 7. \end{cases}$

Упражнение 150. Решите систему $\begin{cases} x_1 x_2 = 1; \\ x_2 x_3 = 1; \\ \dots\dots\dots \\ x_{n-1} x_n = 1; \\ x_n x_1 = 1. \end{cases}$

В следующей системе надо вначале выполнить разложение на множители, потом подходящую линейную замену, после чего система примет вид, аналогичный предыдущим.

Упражнение 151. Решите систему

$$\begin{cases} x^2 = a + (y - z)^2; \\ y^2 = b + (z - x)^2; \\ z^2 = c + (y - x)^2. \end{cases}$$

Переходя к системам общего вида, изложим кратко теоретический метод исключения неизвестных для алгебраических систем с двумя неизвестными. Пусть дана система

$$\begin{cases} f(x, y) = 0; \\ g(x, y) = 0. \end{cases}$$

Будем рассматривать $f(x, y)$ и $g(x, y)$ как многочлены $F(x)$, $G(x)$, коэффициенты которых являются многочленами от y , переменную y можно рассматривать как параметр. Тогда задача решения системы равносильна задаче нахождения значений параметра, при которых многочлены $F(x)$, $G(x)$ имеют общие корни.

Критерием наличия общих корней у двух многочленов является обращение в нуль их *результанта*.

Определение 103. *Результантом* $\text{res}(f, g)$ двух (комплексных) многочленов

$$f(x) = a_n x^n + \dots + a_0, \quad g(x) = b_m x^m + \dots + b_0$$

называется число $a_n^m g(x_1) \dots g(x_n)$, где $x_1, \dots, x_n$ — корни многочлена f с учетом кратности.

Упражнение 152. Докажите формулы

$$\text{res}(f, g) = a_n^m b_m^n \prod_{i=1}^n \prod_{j=1}^m (x_i - y_j) = (-1)^{mn} \text{res}(g, f) = (-1)^{nm} b_m^n f(y_1) \dots f(y_m),$$

где $y_1, \dots, y_m$ — корни многочлена g с учетом кратности.

Из полученных формул сразу следует нужное нам свойство результата: $\text{res}(f, g) = 0 \iff f$ и g имеют общий корень. Но пользы от него никакой, если не уметь вычислять результат, не зная корней многочленов. Оказывается это сделать можно, и многими разными способами.

Самый простой из них для понимания основан на том обстоятельстве, что согласно полученной формуле результат не меняется при любой перестановке корней каждого из этих многочленов, значит, он является

симметрическим многочленом от переменных x_i с коэффициентами, зависящими от y_j , значит, согласно теореме о симметрических многочленах и теореме Виета, он является многочленом от коэффициентов a_i и от корней y_j , причем тоже симметрическим относительно этих корней, поэтому он аналогично может быть выражен не через корни y_j , а через коэффициенты b_j (вместе с коэффициентами a_i).

Упражнение 153. Найдите результат

$$\text{res}(x^2 + p_1x + q_1, x^2 + p_2x + q_2).$$

Указанный алгоритм вычисления результата практически никогда не применяется. Применяются алгоритмы, близкие к разным вариациям алгоритма Евклида, используются различные явные формулы для результата, использующие определители, но мы не можем здесь их излагать.

Выражая $\text{res}(F, G)$ через коэффициенты a_i, b_j многочленов $F(x), G(x)$, получаем многочлен от y . Его степень можно оценить сверху как произведение степеней многочленов $f(x, y), g(x, y)$. Находя его корни и подставляя их в оба уравнения системы, получаем два многочлена с общими корнями, которые можно найти, вычисляя вначале их НОД алгоритмом Евклида. Отсюда можно вывести теорему Безу для случая двух неизвестных.

Упражнение 154. Докажите теорему Безу для систем из двух уравнений с двумя неизвестными, а именно, что такая система либо неопределена и имеет бесконечно много решений, либо имеет не более четырех решений.

Но решать системы из двух уравнений с двумя неизвестными лучше следующим приемом. Применяя подходящее элементарное преобразование, устраняем x^2 из одного из уравнений, и после этого, выражая x через y и подставляя во второе уравнение, получаем уравнение относительно x не выше четвертой степени.

Упражнение 155. Решите систему
$$\begin{cases} x^2 - 2y^2 + 2xy = 1; \\ 2x^2 + y^2 - xy - x + 2y = 3. \end{cases}$$

Задачи и упражнения к § 4.13

Решите системы:

$$1. \begin{cases} x + y + z = a; \\ x^2 + y^2 + z^2 = a^2; \\ x^3 + y^3 + z^3 = a^3. \end{cases} \quad 2. \begin{cases} x + y = a; \\ (x^2 + y^2)(x^3 + y^3) = 2a^5. \end{cases}$$

$$3. \text{ (Кархи, XI в..)} \quad \begin{cases} xy = 10; \\ xz = y^2; \\ x^2 + y^2 = z^2. \end{cases} \quad 4. \quad \begin{cases} \frac{2x^2}{1+x^2} = y; \\ \frac{2y^2}{1+y^2} = z; \\ \frac{2z^2}{1+z^2} = x. \end{cases}$$

$$5. \begin{cases} x_1 + 2x_2 + \dots + 2x_n = 1; \\ x_1 + 3x_2 + 4x_3 + \dots + 4x_n = 2; \\ \dots \\ x_1 + 3x_2 + \dots + (2k-1)x_k + 2kx_{k+1} + \dots + 2kx_n = k; \\ \dots \\ x_1 + 3x_2 + 5x_3 + \dots + (2n-3)x_{n-1} + (2n-1)x_n = n. \end{cases}$$

$$6. \begin{cases} x_1 - 3x_2 + 2x_3 \geqslant 0; \\ x_2 - 3x_3 + 2x_4 \geqslant 0; \\ \\ x_{99} - 3x_{100} + 2x_1 \geqslant 0; \\ x_{100} - 3x_1 + 2x_2 \geqslant 0. \end{cases}$$

[illegible]

§ 4.14. Почему уравнения могут быть неограниченно трудными

Как уже читатель знает, алгебраические и иррациональные уравнения, неравенства и системы представляют не принципиальные, а только технические трудности, так как они могут быть сведены к алгебраическим уравнениям, которые если и не всегда можно решить в радикалах, то по крайней мере можно решить численно сколь угодно точно.

Уравнения *трансцендентные* довольно редко удается свести к алгебраическим, и тогда прибегают к численному решению, например, методом итераций или методом Ньютона.

Покажем, что, вообще говоря, решение трансцендентных уравнений может вызывать принципиальные затруднения. Вначале для простоты

разрешим использовать в уравнениях целую часть $\lfloor x \rfloor$ и получающуюся из нее дробную часть $\{x\} = x - \lfloor x \rfloor$. Рассмотрим систему

$$\left\{ \begin{array}{l} x^y - z^t = 1; \\ x = 4 + x_1^2 + x_2^2 + x_3^2 + x_4^2; \\ y = y_1^2 + y_2^2 + y_3^2 + y_4^2; \\ z = 2 + z_1^2 + z_2^2 + z_3^2 + z_4^2; \\ t = t_1^2 + t_2^2 + t_3^2 + t_4^2; \\ \{x_1\} = 0; \\ \dots\dots\dots \\ \{x_4\} = 0; \\ \{y_1\} = 0; \\ \dots\dots\dots \\ \{y_4\} = 0; \\ \{z_1\} = 0; \\ \dots\dots\dots \\ \{z_4\} = 0; \\ \{t_1\} = 0; \\ \dots\dots\dots \\ \{t_4\} = 0. \end{array} \right.$$

Если эта система имеет решения, то переменные x_i, y_i, z_i, t_i являются целыми числами, а так как согласно теореме Лагранжа о четырех квадратах любое натуральное число представимо в виде суммы четырех квадратов целых чисел, то переменные x, y, z, t при этом могут принимать любые натуральные значения, причем $x \geq 4, z \geq 2$. Поэтому задача сводится к решению в *натуральных числах* уравнения Каталана $x^y - z^t = 1$. Но у этого уравнения, как предположил Каталан и пока еще никто не доказал, есть только одно решение ($x = 3, y = 2, z = 2, t = 3$), которое не удовлетворяет неравенству $x \geq 4$. Поэтому неизвестно, имеет ли данная система решения*.

Конечно, можно написать подобную систему для любого *диофантова уравнения*, т. е. уравнения вида $P(x_1, \dots, x_n) = 0$, где P — произвольный многочлен с целыми коэффициентами, которое тоже надо решать в целых числах. При этом, кстати, можно не использовать теорему Лагранжа и написать более простую систему

$$\left\{ \begin{array}{l} P(x_1, \dots, x_n) = 0; \\ \{x_1\} = 0; \\ \dots\dots\dots \\ \{x_n\} = 0. \end{array} \right.$$

* Сравнительно недавно Тейдеман доказал, что уравнение Каталана имеет конечное число решений.

Многие диофантовы уравнения до сих пор не решены. Более того, в 1970 году аспирант ЛГУ, выпускник ФМШ № 18 при МГУ Юрий Матиясевич* доказал, что проблема распознавания того, имеет ли решения произвольное диофантово уравнение, *алгоритмически неразрешима*. Поэтому и нет алгоритма для решения произвольных трансцендентных систем.

Заметим, что любую систему можно заменить на одно уравнение, так как система

$$\begin{cases} f_1(x_1, \dots, x_n) = 0; \\ \dots\dots\dots \\ f_m(x_1, \dots, x_n) = 0 \end{cases}$$

равносильна уравнению

$$f_1(x_1, \dots, x_n)^2 + \dots + f_m(x_1, \dots, x_n)^2 = 0.$$

Кстати, произвольную систему неравенств

[illegible]

МОЖНО ЗАМЕНИТЬ НА ОДНО УРАВНЕНИЕ

$$(f_1(x_1, \dots, x_n) - y_1^2)^2 + \dots + (f_m(x_1, \dots, x_n) - y_m^2)^2 = 0,$$

содержащее дополнительные неизвестные, но равносильное исходной системе.

Если вам не нравится, что у таких уравнений много неизвестных, то можно все неизвестные $x_i, i = 1, \dots, n$, принимающие натуральные значения, заменить на одно натуральное неизвестное x такое, что $x_i = c_{n,i}(x)$, где $c_{n,i}(x)$ — такие функции, что для любого набора натуральных значений $x_i, i = 1, \dots, n$, найдется единственное натуральное x такое, что $x_i = c_{n,i}(x)$.

Такие функции можно выразить через функцию $\lfloor \sqrt{x} \rfloor$, которую можно, конечно, считать элементарной, если решить следующие упражнения.

Упражнение 156. Докажите, что уравнение

$$c(x, y) = (x + y)(x + y + 1)/2 + x = n,$$

где n — натуральное число, имеет единственное решение в натуральных числах

$$x = c_{2.1}(n) = l(n), \quad y = c_{2.2}(n) = r(n),$$

* Ю. В. Матиясевич (род. 1947), чл.-корр. РАН, профессор матмеха СПбГУ.

где

$$l(n) = n - \frac{1}{2} \left\lfloor \frac{1 + \lfloor \sqrt{8n+1} \rfloor}{2} \right\rfloor \left\lfloor \frac{\lfloor \sqrt{8n+1} \rfloor - 1}{2} \right\rfloor,$$

$$r(n) = \left\lfloor \frac{\lfloor \sqrt{8n+1} \rfloor - 1}{2} \right\rfloor - l(n),$$

значит, эти функции удовлетворяют тождествам $n = c(l(n), r(n))$, $x = l(c(x, y))$, $y = r(c(x, y))$.

У к а з а н и е. Так как

$$2n = (x + y)^2 + 3x + y, \quad 8n + 1 = (2x + 2y + 3)^2 - 8y - 8,$$

выполняются неравенства

$$2x + 2y + 1 \leq \lfloor \sqrt{8n+1} \rfloor < 2x + 2y + 3,$$

$$x + y + 1 \leq \left\lfloor \frac{\lfloor \sqrt{8n+1} \rfloor + 1}{2} \right\rfloor < x + y + 2.$$

Определим по индукции функции

$$c^n(x_1, \dots, x_n) = c^{n-1}(c(x_1, x_2), x_3, \dots, x_n),$$

$$c_{n,1}(x) = l(l \dots l(x) \dots),$$

$$c_{n,2}(x) = r(l(l \dots l(x) \dots)),$$

.....

$$c_{n,n-1}(x) = r(l(x)),$$

$$c_{n,n}(x) = r(x).$$

Упражнение 157. Докажите тождества

$$c^n(c_{n,1}(x), \dots, c_{n,n}(x)) = x, \quad c_{n,i}(c^n(x_1, \dots, x_n)) = x_i.$$

Благодаря этим тождествам можно написать систему с одним неизвестным

$$\begin{cases} P(c_{n,1}(x), \dots, c_{n,n}(x)) = 0; \\ \{x\} = 0, \end{cases}$$

а потом переделать ее в одно уравнение.

Если же вам не нравится использование в этих системах целой части (она хоть и очень простая функция, но все же разрывная), то ее вполне можно заменить синусом, но системы будут немного сложнее.

Упражнение 158. Докажите, что система

$$\begin{cases} P(x_1, \dots, x_n) = 0; \\ \sin(\omega) = 0; \\ \omega > 3; \\ \omega < 4; \\ \sin(\omega x_1) = 0; \\ \dots\dots\dots \\ \sin(\omega x_n) = 0 \end{cases}$$

равносильна диофантову уравнению

$$P(x_1, \dots, x_n) = 0.$$

У к а з а н и е. $\omega = \pi$, поэтому $\sin(\omega x_i) = 0$ означает, что x_i — целое число.

Указанную систему легко заменить на одно уравнение

$$P(x_1, \dots, x_n)^2 + (\omega - 3 - y^2)^2 + (4 - \omega - z^2)^2 + \sin(\omega)^2 + \sin(\omega x_1)^2 + \dots + \sin(\omega x_n)^2 = 0.$$

Можно, но это сложнее, заменить одно уравнение на равносильное уравнение и даже неравенство с одной неизвестной, содержащее кроме арифметических операций только синус.

Задачи и упражнения к § 4.14

1. Если добавить к числу используемых функций $|x|$, то любое неравенство можно заменить на эквивалентное тождество. Поэтому задача распознавания, является ли данное равенство тождеством, алгоритмически неразрешима.

§ 4.15. Алгебра и геометрия

Из этой необозримой темы мы коснемся только вопроса о геометрической интерпретации систем второго порядка. Геометрическую интерпретацию систем первого порядка мы уже рассматривали в § 4.13. Каждое из уравнений такой системы задает на координатной плоскости кривую второго порядка. Решить систему означает найти пересечение этих кривых.

Теорема 106. *Невырожденная кривая второго порядка является либо эллипсом, либо гиперболой, либо параболой. Вырожденная*

кривая является либо объединением двух прямых, либо просто прямой, либо точкой и может быть пустым множеством.

Теорема 107 (Безу). Две кривые второго порядка либо содержат общую прямую, либо имеют не более четырех общих точек.

Мы не будем давать формального доказательства этих теорем, но дадим все же некоторые пояснения.

Определение 104. *Эллипсом* называется множество (или, как писали в старых учебниках, геометрическое место) точек, сумма расстояний от которых до двух данных точек (*фокусов* эллипса) постоянно.

Определение 105. *Гиперболой* называется множество точек, разность расстояний от которых до двух данных точек (*фокусов* гиперболы) постоянна.

Определение 106. *Параболой* называется множество точек, разность расстояний от которых до данной точки (*фокуса* параболы) и данной прямой (*директрисы*, не проходящей через фокус) постоянна.

Эти кривые, известные с глубокой древности, были подробно описаны Аполлонием* в его труде «Конические сечения». Они обладают массой интересных геометрических свойств, которые мы не можем здесь излагать, в частности, они действительно являются сечениями конуса.

Читателю предлагается вслед за Декартом вывести их уравнения.

Упражнение 159. Если провести ось Ox через фокусы эллипса, а ось Oy через его центр (сердину *фокального отрезка*), то уравнение эллипса примет вид

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1.$$

Упражнение 160. Если провести ось Ox через фокусы гиперболы, а ось Oy через его центр (сердину *фокального отрезка*), то ее уравнение примет вид

$$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1.$$

Упражнение 161. Если провести ось Ox через директрису параболы, а ось Oy через ее фокус, то ее уравнение примет вид $y = ax^2$.

Если же выбрать оси координат произвольно, то для этих кривых получатся более сложные уравнения, но они будут уравнениями второго порядка. Верно и обратное.

Для использования геометрической интерпретации в решении систем нужно уметь быстро понимать, какого типа кривую задает каждое уравнение.

* Аполлоний Пергский (Ἀπολλώνιος ὁ Περγαίος, III–II в. до н. э.) — один из великих математиков древности.

Для этого достаточно знать только квадратичную часть уравнения кривой — *квадратичную форму* $ax^2 + 2bxy + cy^2$. Если она нулевая, то кривая вырождается в прямую. В противном случае можно после смены знака считать, что $a > 0$ или эта форма имеет вид $2bxy$. Последний случай можно свести к первому заменой переменных вида

$$\begin{cases} x' = (x + y)/\sqrt{2}; \\ y' = (x - y)/\sqrt{2} \end{cases}$$

(которая геометрически означает поворот системы координат на 45°), так как в новых переменных квадратичная форма примет вид $b(x^2 - y^2)$. Далее выделяем полный квадрат

$$ax^2 + 2bxy + cy^2 = a(x + by/a)^2 + y^2(c - b^2/a)$$

и после замены переменных

$$\begin{cases} x' = x + by/a; \\ y' = y \end{cases}$$

(которая геометрически означает перекося системы координат) квадратичная форма уравнения принимает вид $ax'^2 + by'^2$, а линейная часть уравнения остается линейной. Далее делаем замену переменных

$$\begin{cases} x' = x + c_0; \\ y' = y + c_1 \end{cases}$$

(геометрически означающую параллельный перенос системы координат) и получаем уравнение кривой в виде $ax^2 + by^2 = c$, или в виде $ax^2 = y$, или в виде $ax^2 = c$. В предпоследнем случае кривая является параболой, а в последнем вырождается либо в пару параллельных прямых $x = \pm\sqrt{c/a}$, либо в одну прямую $x = 0$, либо в пустое множество при $c/a < 0$.

В первом случае $a^2 + b^2 > 0$, и если $c = 0$, то кривая вырождается в объединение двух прямых $\sqrt{a}x \pm \sqrt{-b}y = 0$ при $b < 0$ или в точку $(0, 0)$, если $b > 0$. Если же $c \neq 0$, то при $b < 0$ получается гипербола, так как гипербола отличается от эллипса и параболы наличием *асимптот* — прямых, к которым она неограниченно приближается, их не пересекая (в данном случае это прямые $\sqrt{a}x \pm \sqrt{-b}y = 0$), а при $b > 0$ получается либо эллипс, так как эллипс отличается от гиперболы и параболы своей ограниченностью, либо пустое множество, если $c < 0$.

Мы не будем здесь искать *прямоугольную* систему координат, в которой уравнение кривой принимает указанный в упражнениях *канонический* вид, так как для понимания взаимного расположения кривых это не нужно, но рассмотрим более простые и полезные на практике вопросы о том, как быстро рисовать кривые второго порядка для некоторых специальных видов их уравнений.

Для того чтобы быстро нарисовать эскиз параболы $y = ax^2 + bx + c$, не нужно выделять полный квадрат, рисовать параболу $y = x^2$ и сдвигать ее, как учат в различных пособиях. Это все правильно, но медленно. Так как мы уже знаем, что получается парабола, достаточно найти ее три удобные точки, например, $(0, c)$ — точку пересечения с осью ординат, $(1, a + b + c)$, $(-1, a - b + c)$ и плавно провести через них кривую, симметричную относительно прямой $x = -b/2a$. Если у нее есть корни, то лучше их быстро найти подбором по теореме Виета и учесть при проведении кривой. Тогда ось параболы проводится через середину отрезка, соединяющего корни. Направление ветвей параболы (вверх или вниз) определяется только по знаку a .

Упражнение 162. Как по виду графика $y = ax^2 + bx + c$ с данными осями координат определить знаки всех коэффициентов?

Чуть более сложный прием используется для быстрого рисования гиперболы, заданной уравнением вида

$$y = \frac{ax + b}{cx + d}.$$

Для этого сразу рисуются асимптоты $x = -d/c$ (она возникает из-за обращения в нуль знаменателя дроби) и $y = a/c$ (она возникает при стремлении x к бесконечности, так как при больших x указанная дробь приблизительно равна $ax/bx = a/b$) и точки ее пересечения с осями координат $(0, b/d)$, $(-b/a, 0)$. По ним плавно проводятся обе ветви гиперболы.

Упражнение 163. Как по виду графика $y = \frac{ax + b}{cx + d}$ с данными осями координат определить знаки всех коэффициентов?

Если уравнение имеет вид $ax^2 + ay^2 + bx + cy + d = 0$, $a > 0$, то оно задает окружность, точку или пустое множество. Чтобы его нарисовать, нужно преобразовать его к виду $(x - c_0)^2 + (y - c_1)^2 = R^2$, где $c_0 = b/2a$, $c_1 = c/2a$, $R^2 = -(4da + b^2 + c^2)/4a^2$. Окружность имеет центр (c_0, c_1) и радиус R .

Иногда уравнение окружности замаскировано радикалами. От них следует избавиться.

Упражнение 164. Провести через точку $(4, 5)$ касательные к кривой $y = \sqrt{2x - x^2}$.

Особенно полезна геометрическая интерпретация систем уравнений (не обязательно второго порядка) при решении систем и уравнений с параметрами. Если дано одно уравнение с параметром, то полезно нарисовать его как кривую на плоскости — в этом заключается идея так называемого «метода *Оха*».

Упражнение 165. Решите уравнение с параметром $x^2 + 2ax + 5a^2 - 4a - 8 = 0$.

Упражнение 166. При каких a система $\begin{cases} x^2 + y^2 = 1; \\ ax + y = 1 \end{cases}$ имеет решение?

Можно изображать на плоскости и системы неравенств.

Упражнение 167. Найдите все a , при которых разрешима система

$$\begin{cases} x^2 + 4x + 3 + a < 0; \\ 2x + a + 6 > 0. \end{cases}$$

Полезно для этого разложить их левые части на множители.

Упражнение 168. Нарисовать на плоскости решение системы неравенств

$$\begin{cases} (x^2 + y^2 - 1)(x - y) < 0; \\ (x^2 + 4y^2 - 4)(xy - 1) > 0. \end{cases}$$

Задачи и упражнения к § 4.15

1. Докажите, что все параболы $y = ax^2 + bx + c$ подобны друг другу (в элементарно-геометрическом смысле).

2. Докажите, что все гиперболы $y = \frac{ax + b}{cx + d}$ подобны друг другу.

3. Эллипсы могут быть не подобными друг другу. Гиперболы, вообще говоря, тоже.

4. Парабола $y = ax^2 + bx + c$ однозначно определяется любыми тремя своими точками. Гипербола $y = \frac{ax + b}{cx + d}$ тоже.

5. Произвольная кривая второго порядка однозначно определяется любыми пятью своими точками.

6. При каких a система

$$\begin{cases} x^2 + 2xy - 7y^2 \geq \frac{1-a}{1+a}; \\ 3x^2 + 10xy - 5y^2 \leq -2 \end{cases}$$

имеет решение?

Еще одной причиной, почему эта функция заслуживает звания комплексной экспоненты, служит то, что при действительном z она совпадает с действительной экспонентой: $e^z = e^x e^{0i} = e^x$.

И третья причина в том, что, как и в действительном случае, $\lim_{z \rightarrow 0} \frac{e^z - 1}{z} = 1$, но мы не будем здесь это доказывать.

Не будем также доказывать, что указанные тождество и предел однозначно определяют удовлетворяющую им функцию как в комплексном, так и в действительном случаях.

Заметим, что из формулы $e^{ix} = \cos x + i \sin x$ следуют соотношения

$$\sin x = \frac{e^{ix} - e^{-ix}}{2i}, \quad \cos x = \frac{e^{ix} + e^{-ix}}{2}.$$

Заменяя в них x на комплексную переменную z , можно распространить эти функции на комплексную плоскость равенствами

$$\sin z = \frac{e^{iz} - e^{-iz}}{2i}, \quad \cos z = \frac{e^{iz} + e^{-iz}}{2}.$$

Читателю предлагается убедиться в том, что теоремы сложения справедливы и в комплексном случае, причем выводятся они из теоремы сложения для комплексной экспоненты даже проще, чем тригонометрические теоремы сложения в действительном случае.

Упражнение 169. Докажите тождества

- а) $\sin(z_1 + z_2) = \sin z_1 \cos z_2 + \cos z_1 \sin z_2$,
 $\cos(z_1 + z_2) = \cos z_1 \cos z_2 - \sin z_1 \sin z_2$;
 б) $\cos^2 z + \sin^2 z = 1$.

Можно доказать также в комплексном случае и замечательный предел

$$\lim_{z \rightarrow 0} \frac{\sin z}{z} = 1,$$

а также тот факт, что три предыдущих равенства и этот предел однозначно определяют тригонометрические функции как в комплексном, так и в действительном вариантах, но мы здесь не будем это делать.

Гиперболические функции тоже могут быть распространены на комплексную область. Для этого используем формулы

$$\operatorname{sh} z = \frac{e^z - e^{-z}}{2}, \quad \operatorname{ch} z = \frac{e^z + e^{-z}}{2}.$$

Для них теоремы сложения и связи между функциями также переносятся в комплексную область, причем без изменений в доказательствах.

Упражнение 170. Докажите тождества

$$а) \operatorname{sh}(z_1 + z_2) = \operatorname{sh} z_1 \operatorname{ch} z_2 + \operatorname{ch} z_1 \operatorname{sh} z_2,$$

$$\operatorname{ch}(z_1 + z_2) = \operatorname{ch} z_1 \operatorname{ch} z_2 + \operatorname{sh} z_1 \operatorname{sh} z_2;$$

$$б) \operatorname{ch}^2 z - \operatorname{sh}^2 z = 1.$$

Одной из важнейших идей в математике является обращение функций и операций. В результате обращения сложения получилось вычитание и вслед за ним — отрицательные числа. В результате обращения умножения получилось деление и вслед за ним — рациональные числа. Обращением степенной функции с натуральным показателем получились квадратные и прочие корни и т. д.

Попробуем обратить комплексную экспоненту e^z . Обратная функция к действительной экспоненте нам известна — это натуральный логарифм $\ln x$. Для обращения комплексной экспоненты надо решать уравнение $e^w = z \neq 0$ относительно неизвестной $w = x + iy$. Так как

$$z = e^{x+iy} = e^x (\cos y + \sin iy), \quad |z| = e^x, \quad \arg z = y \bmod 2\pi,$$

то $x = \ln |z|$, $y = y_k = \arg z + 2\pi k$, $k \in \mathbb{Z}$. Получилась бесконечная серия решений

$$\omega_k = \omega_0 + 2\pi ki, \quad k \in \mathbb{Z}, \quad \omega_0 = \ln |z| + i \arg z,$$

что не удивительно, так как комплексная экспонента имеет период $2\pi i$, действительно, справедливо тождество $e^{z+2\pi i} = e^z$.

Функцию, принимающую значение ω_0 , естественно обозначить $\operatorname{Ln} z$. Ясно, что при действительном положительном z она совпадает с обычным действительным логарифмом.

Но как быть с остальными значениями? По причинам, которые здесь нет возможности объяснять, удобно ввести в рассмотрение функцию $\operatorname{Ln} z$, принимающую бесконечное множество значений ω_k — *бесконечнозначную* функцию. Строгая теория таких функций сложна, и мы не можем излагать ее здесь.

Но если читателю неприятно иметь дело с многозначной функцией, ее можно превратить в однозначную, но принимающую в качестве значений не комплексные числа, а *классы эквивалентности* таких чисел по модулю $2\pi i$.

Определение 108. Числа z, w назовем *эквивалентными по модулю $2\pi i$* (обозначение $z = w \bmod 2\pi i$), если $z - w = 2\pi ki$, $k \in \mathbb{Z}$. *Классом эквивалентности числа z* назовем множество всех эквивалентных ему чисел (обозначение $z \bmod 2\pi i$). Множество всех таких *классов эквивалентности* обозначим G . Множество *классов эквивалентности действительных чисел по модулю 2π* обозначим $\mathbb{T}$.

На введенных множествах можно определить операции сложения, и они превратятся в группы.

Определение 109. Пусть даны $A = a \bmod 2\pi i$ и $B = b \bmod 2\pi i$ — два класса эквивалентности. Назовем *суммой* $A + B$ тот класс эквивалентности, который содержит число $a + b$, т. е. $(a + b) \bmod 2\pi i$.

Для обоснования корректности этого определения понадобится

Упражнение 171. Если $a \bmod 2\pi i = c \bmod 2\pi i$ и $b \bmod 2\pi i = d \bmod 2\pi i$, то $(a + b) \bmod 2\pi i = (c + d) \bmod 2\pi i$.

В следующем упражнении проверяется, что множество $R \times T$ с введенной операцией сложения образует *коммутативную группу*.

Упражнение 172. Проверьте, что введенная операция сложения обладает свойствами ассоциативности и коммутативности, нулевым классом относительно этого сложения является класс $0 \bmod 2\pi i$, а также справедливо равенство

$$(-a \bmod 2\pi i) + (a \bmod 2\pi i) = 0 \bmod 2\pi i.$$

Аналогичным образом определяется коммутативная группа и на множестве T .

Раньше мы уже проверяли, что и поле действительных чисел $\mathbb{R}$ относительно операции сложения образует коммутативную группу.

Теорема 108. *Группа G изоморфна прямому произведению групп $\mathbb{R}$ и T , т. е. группе $\mathbb{R} \times T$.*

Доказательство. Сопоставим произвольному классу $z \bmod 2\pi i$ из группы G упорядоченную пару $(\operatorname{Re} z, \operatorname{Im} z \bmod 2\pi)$, первая компонента которой есть действительное число $\operatorname{Re} z$, а вторая — класс эквивалентности по модулю 2π , содержащий действительное число $\operatorname{Im} z$. Тогда

$$(\operatorname{Re} z, \operatorname{Im} z \bmod 2\pi) \in \mathbb{R} \times T.$$

Указанное соответствие является взаимно однозначным соответствием между группами G и $\mathbb{R} \times T$.

Так как для любых комплексных чисел z_1, z_2

$$\operatorname{Re}(z_1 + z_2) = \operatorname{Re} z_1 + \operatorname{Re} z_2, \quad \operatorname{Im}(z_1 + z_2) = \operatorname{Im} z_1 + \operatorname{Im} z_2,$$

$$\begin{aligned} \operatorname{Im}(z_1 + z_2) \bmod 2\pi &= (\operatorname{Im} z_1 + \operatorname{Im} z_2) \bmod 2\pi = \\ &= (\operatorname{Im} z_1 \bmod 2\pi) + (\operatorname{Im} z_2 \bmod 2\pi), \end{aligned}$$

то сумме классов $(z_1 + z_2) \bmod 2\pi$ будет сопоставляться упорядоченная пара $(\operatorname{Re} z_1 + \operatorname{Re} z_2, (\operatorname{Im} z_1 \bmod 2\pi) + (\operatorname{Im} z_2 \bmod 2\pi))$, которая, по определению сложения в прямом произведении групп $\mathbb{R}$ и T , равна сумме

$$(\operatorname{Re} z_1, \operatorname{Im} z_1 \bmod 2\pi) + (\operatorname{Re} z_2, \operatorname{Im} z_2 \bmod 2\pi),$$

что и доказывает объявленный изоморфизм. $\square$

Теперь мы можем рассматривать функцию $\text{Ln } z$ как отображение из группы ненулевых комплексных чисел относительно умножения (*мультипликативной группы*) в группу $\mathbb{R} \times \mathbb{T}$. Значение $\text{Ln } z$ определим как $\text{Ln } z = \ln z \bmod 2\pi i = (\ln |z|, \arg z \bmod 2\pi)$. При этом справедливо логарифмическое тождество $\text{Ln}(z_1 z_2) = \text{Ln } z_1 + \text{Ln } z_2$. Действительно, если $\ln z_i = \omega_i$, то $e^{\omega_i} = z_i$, значит, $e^{\omega_1 + \omega_2} = e^{\omega_1} e^{\omega_2} = z_1 z_2 \neq 0$, откуда

$$\begin{aligned} \text{Ln}(z_1 z_2) &= \ln(z_1 z_2) \bmod 2\pi i = (\omega_1 + \omega_2) \bmod 2\pi i = \\ &= (\omega_1 \bmod 2\pi i) + (\omega_2 \bmod 2\pi i) = \\ &= (\ln z_1 \bmod 2\pi i) + (\ln z_2 \bmod 2\pi i) = \text{Ln } z_1 + \text{Ln } z_2. \end{aligned}$$

Упражнение 173. Проверьте, что единичная окружность на комплексной плоскости $|z| = 1$ относительно операции умножения образует группу.

Функция e^{ix} отображает действительную ось (группу $\mathbb{R}$ относительно сложения) в эту группу, причем справедливо тождество

$$e^{i(x_1 + x_2)} = e^{ix_1} e^{ix_2}.$$

Это отображение не взаимно однозначно, поэтому оно не является изоморфизмом этих групп (и они действительно не изоморфны). Но отображение $x \bmod 2\pi \rightarrow e^{ix}$ из группы $\mathbb{T}$ в единичную окружность корректно определено, взаимно однозначно и является изоморфизмом указанных групп, так как

$$(x \bmod 2\pi) + (y \bmod 2\pi) = (x + y) \bmod 2\pi \rightarrow e^{i(x+y)} = e^{ix} e^{iy}.$$

Тем самым доказана

Теорема 109. *Мультипликативная группа комплексных чисел, по модулю равных единице, изоморфна группе $\mathbb{T}$ действительных чисел по модулю 2π относительно сложения.*

На самом деле, конечно, в этой формулировке можно заменить 2π на любое положительное число.

Доказанная теорема кажется очевидной, но в ней фактически замаскирована вся тригонометрия, а строгого построения теории тригонометрических функций мы не давали. Если же попытаться доказать эту теорему, не пользуясь тригонометрическими функциями, то это станет трудной задачей, по существу эквивалентной строгому построению тригонометрии.

Обратные тригонометрические функции можно определить аналогичным логарифму образом, и они тоже оказываются бесконечнозначными. Но так как тригонометрические функции выражаются через экспоненту, то и обратные к ним функции можно выразить через комплексный логарифм.

Упражнение 174. Докажите тождества

- а) $\arcsin z = -i \operatorname{Ln} (iz + \sqrt{1 - z^2})$; б) $\arccos z = -i \operatorname{Ln} (z + \sqrt{z^2 - 1})$;
 в) $\operatorname{arctg} z = \frac{i}{2} \operatorname{Ln} \frac{1 - iz}{1 + iz}$.

Функции, обратные к гиперболическим, можно выразить через логарифмы, не используя мнимую единицу.

Упражнение 175. Докажите тождества

- а) $\operatorname{Arsh} z = \operatorname{Ln} (z + \sqrt{1 + z^2})$; б) $\operatorname{Arch} z = \operatorname{Ln} (z + \sqrt{z^2 - 1})$;
 в) $\operatorname{Arth} z = \frac{1}{2} \operatorname{Ln} \frac{1 + z}{1 - z}$.

С помощью логарифма можно определить и комплексную степенную функцию. Для любых комплексных $A \neq 0$, B положим по определению $A^B = e^{B \operatorname{Ln} A}$. Эта функция также будет, разумеется, бесконечнозначной.

Но если A — действительное положительное, то A^z можно считать однозначной функцией $e^{z \operatorname{Ln} A}$. Обратная к A^z функция $\operatorname{Log}_A z = \frac{\operatorname{Ln} z}{\operatorname{Ln} A}$ будет, естественно, бесконечнозначной.

Примеры. 1. Справедливо равенство $e^{\pi i} = -1$. Эта формула Эйлера символизирует единство всей математики. Число e представляет в ней анализ, i — алгебру, -1 — арифметику, а π — геометрию. С определенной точки зрения она представляет собой скорее определение, чем теорему.

2. Справедливо равенство $(-1)^i = e^{\pi(1+2k)i}$, $k \in \mathbb{Z}$. Действительно, $e^{\pi(1+2k)i} = -1$, значит, $\operatorname{Ln}(-1) = \pi(1+2k)i$, откуда

$$(-1)^i = e^{i \operatorname{Ln}(-1)} = e^{-\pi(1+2k)} = e^{\pi(1+2k)}$$

имеет бесконечную серию действительных значений. Главное из них e^π . Трансцендентность (т. е. неалгебраичность) этого числа впервые доказал в 1929 г. аспирант МГУ А. О. Гельфонд, решив тем самым седьмую проблему Гильберта.

Задачи и упражнения к § 4.16

1. Вычислите $\sqrt[i]{-1}$.
2. Определите в комплексной области тангенс, проверьте, что на действительной оси он совпадает с обычным тангенсом, и докажите для него теорему сложения.
3. Докажите для комплексных тригонометрических функций формулы приведения и свойства четности-нечетности.
4. Найдите периоды комплексных тригонометрических функций и убедитесь, что они такие же, как и у действительных.

5. Комплексная экспонента, в отличие от действительной, — периодическая функция. Ее период равен $2\pi i$. Гиперболические функции тоже периодические с периодом $2\pi i$.

6. Докажите формулы, связывающие друг с другом разные тригонометрические функции.

7. Покажите, что любая (в разумном понимании) формула действительной тригонометрии справедлива и в комплексной тригонометрии.

8. Докажите, что

$$\begin{aligned}\sin(x + yi) &= \sin x \operatorname{ch} y + i \cos x \operatorname{sh} y, \\ \cos(x + yi) &= \cos x \operatorname{ch} y - i \sin x \operatorname{sh} y.\end{aligned}$$

9. Докажите формулы связи между обычными и гиперболическими функциями

$$\operatorname{sh} iz = i \sin z, \quad \operatorname{ch} iz = \cos z, \quad \sin iz = i \operatorname{sh} z, \quad \cos iz = \operatorname{ch} z.$$

10. Выведите с помощью этих формул связи из тригонометрических теорем сложения гиперболические теоремы сложения и наоборот.

11. Докажите, что

$$\begin{aligned}\operatorname{sh}(x + yi) &= \operatorname{sh} x \cos y + i \operatorname{ch} x \sin y, \\ \operatorname{ch}(x + yi) &= \operatorname{ch} x \cos y + i \operatorname{sh} x \sin y.\end{aligned}$$

12*. Определим функцию (называемую *гудерманианом*)

$$\operatorname{gd} z = 2 \operatorname{arctg} e^z - \frac{\pi}{2}.$$

Докажите, что если $w = \operatorname{gd} z$, то $z = \operatorname{Ln} \left(\operatorname{tg} \left(\frac{w}{2} + \frac{\pi}{4} \right) \right)$, и

$$\begin{aligned}\operatorname{sh} z &= \operatorname{tg} w, & \operatorname{ch} z &= \sec w, & \operatorname{th} z &= \sin w, \\ \operatorname{cth} z &= \operatorname{cosec} w, & \operatorname{csch} z &= \operatorname{ctg} w, & \operatorname{sch} z &= \cos w\end{aligned}$$

(гиперболические функции переходят в тригонометрические и наоборот!).

§ 4.17. Тригонометрические многочлены

Определение 110. Назовем *тригонометрическим многочленом* степени n (или порядка n) выражение вида

$$a_0 + (a_1 \sin z + b_1 \cos z) + \dots + (a_n \sin nz + b_n \cos nz).$$

Если его коэффициенты a_i , b_i комплексные, то тригонометрический многочлен называем *комплексным*, а если они действительные, то его называем *действительным*, при этом естественно предполагать, что

и переменная z действительная, и обозначать ее x . Предполагаем также, что $a_n \neq 0$ или $b_n \neq 0$.

Для того чтобы дать еще два эквивалентных определения тригонометрических многочленов, понадобится интересная и сама по себе лемма.

Лемма 27. *Справедливы тождества:*

$$\begin{aligned} \text{(i)} \quad \sin nz &= \frac{e^{inz} - e^{-inz}}{2i} \sum_{k=0}^{\lfloor (n-1)/2 \rfloor} C_n^{2k+1} (-1)^k \sin^{2k+1} z \cos^{n-2k-1} z; \\ \text{(ii)} \quad \cos nz &= \frac{e^{inz} + e^{-inz}}{2} \sum_{k=0}^{\lfloor n/2 \rfloor} C_n^{2k} (-1)^k \sin^{2k} z \cos^{n-2k} z; \\ \text{(iii)} \quad \sin^n z \cos^m z &= \left(\frac{e^{iz} - e^{-iz}}{2i} \right)^n \left(\frac{e^{iz} + e^{-iz}}{2} \right)^m = \sum_{k=-n-m}^{k=n+m} c_k e^{ikz} = \\ &= \sum_{k=0}^{k=n+m} a_k \sin kz + b_k \cos kz, \end{aligned}$$

где коэффициенты a_k, b_k будут действительными и $a_{n+m}^2 + b_{n+m}^2 > 0$.

Доказательство. Для доказательства (i) используем формулу Муавра

$$\sin nz = \frac{e^{inz} - e^{-inz}}{2i} = \frac{(\cos z + i \sin z)^n - (\cos z - i \sin z)^n}{2}$$

и далее два раза формулу бинома, учитывая, что в них четные слагаемые сокращаются, а нечетные слагаемые удваиваются, и заменяя в них i^{2k+1} на $i(-1)^k$.

Формула (ii) доказывается аналогично, только в ней при раскрытии биномов сокращаются нечетные слагаемые.

Для доказательства формулы (iii) достаточно раскрыть скобки в сомножителях

$$\left(\frac{e^{iz} - e^{-iz}}{2i} \right)^n \left(\frac{e^{iz} + e^{-iz}}{2} \right)^m$$

по формулам бинома, а потом заменить каждое слагаемое $c_k e^{ikz}$ на $a_k \sin kz + b_k \cos kz$. Ясно, что $c_{n+m} \neq 0$.

Заметим, что при замене в обоих сомножителях i на $-i$ оба они не меняются, а значит, не меняется и их произведение, но представление его в виде

$$\sum_{k=-n-m}^{k=n+m} c_k e^{ikz}$$

единственно согласно известному свойству полиномиальных функций. Следовательно, сумма $c_k e^{ikz} + c_{-k} e^{-ikz}$ не меняется при замене i на $-i$.

При этой замене c_j превращается в комплексно-сопряженное $\overline{c_j}$, поэтому c_k и c_{-k} сопряжены друг другу, т. е.

$$c_k = A_k + iB_k, \quad c_{-k} = A_k - iB_k,$$

значит,

$$\begin{aligned} c_k e^{ikz} + c_{-k} e^{-ikz} &= 2 \operatorname{Re} c_k e^{ikz} = \\ &= 2 \operatorname{Re} (A_k + iB_k)(\cos kz + i \sin kz) = 2(A_k \cos kz - B_k \sin kz) \end{aligned}$$

и остается сложить полученные равенства. $\square$

Из этой леммы легко следует

Теорема 110 (о тригонометрических многочленах).

(i) Любой тригонометрический многочлен степени n можно представить единственным образом в виде

$$c_{-n} e^{-inz} + \dots + c_{-1} e^{-iz} + c_0 + c_1 e^{iz} + \dots + c_n e^{inz} = e^{-inz} P_{2n}(e^{iz}),$$

где P_{2n} — многочлен степени не выше $2n$, а в действительном случае — многочлен в точности степени $2n$, коэффициенты которого удовлетворяют равенствам $c_k = \overline{c_{-k}}$, и обратно, любое выражение $e^{-inz} P_{2n}(e^{iz})$, где P_{2n} — многочлен степени $2n$, представимо единственным образом в виде тригонометрического многочлена степени n , а если коэффициенты многочлена удовлетворяют равенствам $c_k = \overline{c_{-k}}$, то тригонометрический многочлен имеет действительные коэффициенты.

Для любого действительного тригонометрического многочлена степени n соответствующий многочлен $P_{2n}(z)$ удовлетворяет тождеству

$$\overline{P_{2n}(z)} = \overline{z}^{2n} P_{2n}(1/\overline{z})$$

и его корни, отличные от нуля и единицы, распадаются на пары вида $(z_i, 1/\overline{z_i})$.

(ii) Любой тригонометрический многочлен степени n можно представить (но не единственным образом) в виде многочлена от $\sin x$, $\cos x$ степени n

$$\sum_{i+j \leq n} c_{i,j} \sin^i x \cos^j x,$$

и обратно, любой многочлен от $\sin x$, $\cos x$ степени n представим единственным образом в виде тригонометрического многочлена степени n , причем действительный тригонометрический многочлен представим в виде действительного многочлена от $\sin x$, $\cos x$.

Доказательство. Для представления тригонометрического многочлена степени n в виде дроби $e^{-inz}P_{2n}(e^{iz})$ или в виде $Q_n(\sin z, \cos z)$, где $Q_n(x, y)$ — многочлен степени n , достаточно воспользоваться формулами (i), (ii) предыдущей леммы, умножить их на коэффициенты a_k, b_k и сложить, добавив еще константу a_0 .

Первое утверждение о действительных тригонометрических многочленах вытекает из равенства

$$\begin{aligned} c_k e^{ikz} + \overline{c_k} e^{-ikz} &= 2 \operatorname{Re} c_k e^{ikz} = \\ &= 2 \operatorname{Re}(A_k + iB_k)(\cos kz + i \sin kz) = 2(A_k \cos kz - B_k \sin kz). \end{aligned}$$

Докажем однозначность представления в виде тригонометрического многочлена и в виде дроби. Из соотношения

$$a_n \sin nz + b_n \cos nz = \frac{a_n i + b_n}{2} e^{inz} + \frac{a_n i - b_n}{2} e^{-inz}$$

следует, что если a_n, b_n одновременно не равны нулю, то в многочлене P_{2n} свободный член и старший коэффициент одновременно не равны нулю, поэтому ненулевой тригонометрический многочлен представляется в виде $e^{-inz}P_{2n}(e^{iz})$, где P_{2n} — ненулевой многочлен степени не выше $2n$. Так как ненулевой многочлен над полями нулевой характеристики имеет конечное число корней, ненулевой тригонометрический многочлен реализует ненулевую функцию, поэтому представление в виде тригонометрического многочлена обладает свойством единственности.

Если же a_n, b_n действительны, то $a_n i + b_n \neq 0$, и поэтому степень многочлена P_{2n} равна в точности $2n$.

Последнее утверждение о действительных тригонометрических многочленах вытекает из соотношений $\overline{c_k} = c_{-k}$ и свойства операции сопряжения.

Для обратного преобразования можно воспользоваться формулами (iii) предыдущей леммы

$$\sin^n z \cos^m z = \sum_{k=-n-m}^{k=n+m} c_k e^{ikz} = \sum_{k=0}^{k=n+m} (a_k \sin kz + b_k \cos kz),$$

умножить их на подходящие коэффициенты и сложить, добавив еще константу a_0 .

Единственности для представления в виде $Q_n(\sin z, \cos z)$, естественно, быть не может в силу тождества $\sin^2 z + \cos^2 z = 1$. Но разные представления должны иметь одинаковую степень, так как в противном случае разные тригонометрические многочлены реализуют одинаковые функции. $\square$

Упражнение 176. Докажите, что произведение тригонометрических многочленов порядков n и m есть тригонометрический многочлен порядка $n + m$.

Напомним, что функция называется четной, если она не меняется при смене знака у переменной, и нечетной, если она при этом меняет знак.

Упражнение 177. Тригонометрический многочлен четен тогда и только тогда, когда он состоит из одних косинусов, и нечетен, если он состоит только из синусов.

Лемма 28. *Справедливы тождества:*

$$\begin{aligned} \text{(i)} \quad \sin nx &= \sin x \cdot U_{n-1}(\cos x) = \\ &= \sin x \sum_{k=0}^{\lfloor (n-1)/2 \rfloor} C_n^{2k+1} (-1)^k (1 - \cos^2 x)^k \cos^{n-2k-1} x; \\ \text{(ii)} \quad \cos nx &= T_n(\cos x) = \sum_{k=0}^{\lfloor n/2 \rfloor} C_n^{2k} (-1)^k (1 - \cos^2 x)^k \cos^{n-2k} x, \end{aligned}$$

причем действительные многочлены T_n и U_{n-1} степеней n и $n-1$ определяются однозначно.

Доказательство. Существование многочленов T_n и U_{n-1} , удовлетворяющих указанным тождествам, следует из формул (i), (ii) предыдущей леммы. Единственность вытекает из п. (i) предыдущей теоремы. $\square$

Многочлены T_n и U_{n-1} называются *многочленами Чебышёва первого и второго рода* соответственно.

Теорема 111 (о четных и нечетных тригонометрических многочленах). (i) *Любой четный тригонометрический многочлен степени n можно представить единственным образом в виде многочлена от $\cos z$ степени n , и обратно, любой многочлен от $\cos z$ степени n представим единственным образом в виде четного тригонометрического многочлена степени n , причем действительному тригонометрическому многочлену соответствует действительный многочлен от $\cos z$.*

(ii) *Любой нечетный тригонометрический многочлен степени n можно представить единственным образом в виде многочлена от $\cos z$ степени $n-1$, умноженного на $\sin z$, и обратно, любой многочлен от $\cos z$ степени $n-1$, умноженный на $\sin z$, представим единственным образом в виде нечетного тригонометрического многочлена степени n , причем действительному тригонометрическому многочлену соответствует действительный многочлен от $\cos z$.*

Доказательство. Существование многочленов в п. (i), (ii) вытекает из п. (i), (ii) предыдущей леммы. Для доказательства существования обратного преобразования достаточно заметить, что

$$\cos^n x - A \sin(n+1)x / \sin x \quad \text{и} \quad \cos^n x - B \cos nx$$

при подходящих A, B являются многочленами от $\cos x$ степени, меньшей $n-1$, и применить индукцию.

Единственность вытекает из того, что два многочлена с действительными коэффициентами совпадают, если они принимают равные значения на бесконечном множестве точек. $\square$

Так как тригонометрические многочлены реализуют функции с периодом 2π , естественно считать у них корни с точностью до эквивалентности по модулю 2π , т.е. два корня z_1 и z_2 считаем эквивалентными, если $z_1 \equiv z_2 \pmod{2\pi}$. Кратностью корня тригонометрического многочлена назовем кратность этого же корня у соответствующего этому тригонометрическому многочлену алгебраического многочлена вдвое большей степени.

Теорема 112 (о числе корней тригонометрических многочленов).

(i) *Комплексный тригонометрический многочлен степени n имеет не более $2n$ комплексных корней с учетом кратности.*

(ii) *Действительный тригонометрический многочлен степени n имеет не более $2n$ действительных корней с учетом кратности.*

Доказательство. Для доказательства достаточно воспользоваться представлением тригонометрического многочлена степени n в виде $e^{-inz} P_{2n}(e^{iz})$ и заметить, что $e^{-inz} \neq 0$. $\square$

Предыдущая теорема полезна при решении тригонометрических уравнений, большинство из которых сводится к поиску корней действительных тригонометрических многочленов. Доказательство этой теоремы дает и метод поиска корней: сведение к алгебраическому уравнению $P_{2n}(e^{iz})$, отбору его корней, имеющих модуль, равный единице, и нахождению их аргументов.

Иногда удобнее не использовать явно комплексные числа, а воспользоваться представлением тригонометрического многочлена в виде $Q_n(\cos x, \sin x)$ и выразить, например, $\sin x$ через $\cos x$, что потребует, однако, избавления от появившегося радикала путем возведения в квадрат и приведет к удвоению степени уравнения.

Можно избежать указанной процедуры, если применить так называемую универсальную подстановку, выражающую $\sin x$ и $\cos x$ через $\operatorname{tg}(x/2)$. При этом степень получившегося уравнения относительно $\operatorname{tg}(x/2)$ также удваивается.

Упражнение 178. Проверьте формулы

$$\text{а) } \sin x = \frac{2 \operatorname{tg}(x/2)}{1 + \operatorname{tg}^2(x/2)}; \quad \text{б) } \cos x = \frac{1 - \operatorname{tg}^2(x/2)}{1 + \operatorname{tg}^2(x/2)}.$$

В некоторых случаях, например, когда многочлен $Q_n(\cos x, \sin x)$ однородный, т. е. состоит только из одночленов вида $\sin^k x \cos^{n-k} x$, соответствующее уравнение можно свести к уравнению относительно $\operatorname{tg} x$, не повышая при этом его степени.

Если тригонометрический многочлен четный или нечетный, то соответствующее уравнение можно свести к уравнению относительно $\cos x$, не повышая при этом его степени.

Задачи и упражнения к § 4.17

Задачи в этом параграфе, как правило, трудны, но они становятся вполне доступными, если решать их в частных случаях $n = 2, 3, 4, \dots$

Первый цикл задач посвящен многочленам Чебышёва. Подобных задач известно колоссальное количество, и мы здесь приводим только некоторые из них.

1. Докажите рекуррентные соотношения и проверьте начальные условия

$$\begin{aligned} T_n(x) &= 2xT_{n-1}(x) - T_{n-2}(x), & T_0(x) &= 1, & T_1(x) &= x, \\ U_n(x) &= 2xU_{n-1}(x) - U_{n-2}(x), & U_0(x) &= 1, & U_1(x) &= 2x. \end{aligned}$$

2. Эти последовательности можно продолжить и для отрицательных индексов. Докажите соотношения $T_n = T_{-n}$, $U_n = -U_{-n-2}$.

3. Докажите при $n \neq -1$ тождество

$$U_n(x) = \frac{1}{n+1} T'_{n+1}(x).$$

4. Докажите тождества:

$$\text{а) } T_n(-x) = (-1)^n T_n(x); \quad \text{б) } U_n(-x) = (-1)^n U_n(x).$$

5. Докажите равенства:

$$\begin{aligned} \text{а) } T_n(x) &= \sum_{k=0}^{\lfloor n/2 \rfloor} C_n^{2k} x^{n-2k} (x^2 - 1)^k; \\ \text{б) } U_n(x) &= \sum_{k=0}^{\lfloor n/2 \rfloor} C_{n+1}^{2k+1} x^{n-2k} (x^2 - 1)^k; \end{aligned}$$

$$\text{в)} \quad T_n(x) = \frac{n}{2} \sum_{k=0}^{\lfloor n/2 \rfloor} \frac{(-1)^k}{n-k} C_{n-k}^k (2x)^{n-2k};$$

$$\text{г)} \quad U_n(x) = \sum_{k=0}^{\lfloor n/2 \rfloor} (-1)^k C_{n-k}^k (2x)^{n-2k}.$$

6. Докажите при $|x| < 1$ тождества:

$$\text{а)} \quad T_n(x) = \cos(n \arccos x);$$

$$\text{б)} \quad U_n(x) = \sin((n+1) \arccos x) / \sin(\arccos x).$$

7*. Докажите при $|x| > 1$ тождества:

$$\text{а)} \quad T_n(x) = \frac{1}{2}((x + \sqrt{x^2 - 1})^n + (x - \sqrt{x^2 - 1})^n);$$

$$\text{б)} \quad T_n(x) = \operatorname{ch}(n \operatorname{Arch} x);$$

$$\text{в)} \quad U_n(x) = \frac{1}{2\sqrt{x^2 - 1}}((x + \sqrt{x^2 - 1})^{n+1} + (x - \sqrt{x^2 - 1})^{n+1});$$

$$\text{г)} \quad U_n(x) = \operatorname{sh}((n+1) \operatorname{Arch} x) / \operatorname{sh}(\operatorname{Arch} x).$$

8. Найдите корни и экстремумы многочленов Чебышёва первого и второго рода.

9. Докажите рекуррентные соотношения:

$$\text{а)} \quad T_m T_n = \frac{1}{2}(T_{m-n} + T_{m+n});$$

$$\text{б)} \quad U_m T_n = \frac{1}{2}(U_{m-n} + U_{m+n});$$

$$\text{в)} \quad T_m(x) T_n(x) \pm (1 - x^2) U_{m-1} U_{n-1}(x) = T_{m \mp n}(x);$$

$$\text{г)} \quad U_{m-1}(x) T_n(x) \pm T_m U_{n-1}(x) = U_{m \pm n-1}(x);$$

$$\text{д)} \quad T_m(T_n) = T_{mn}(x);$$

$$\text{е)} \quad U_{m-1}(T_n) = U_{mn-1}/U_{n-1};$$

$$\text{ж)} \quad T_n = \frac{1}{2}(U_n - U_{n-2});$$

$$\text{з)} \quad T_n(x) = U_n(x) - x U_{n-1};$$

$$\text{и)} \quad T_n(x) = x U_{n-1}(x) - U_{n-2}.$$

10**. Докажите, что сложность совместного вычисления значений $T_n(x)$, $U_n(x)$ не больше $C \log_2 n$, где C — константа.

11*. Для любого тригонометрического многочлена

$$t_n(x) = a_0 + \sum_{k=1}^n (a_k \cos kx + b_k \sin kx)$$

при $n \geq m > n/3$ справедливо тождество

$$\begin{aligned} t_n(x) - t_n\left(x + \frac{\pi}{m}\right) + t_n\left(x + \frac{2\pi}{m}\right) - \dots - t_n\left(x + \frac{\pi(2m-1)}{m}\right) = \\ = a_m \cos mx + b_m \sin mx. \end{aligned}$$

12*. Назовем *нормой* и обозначим $\|t_n\|$ максимум модуля тригонометрического многочлена t_n . Докажите для любого m , $n \geq m > n/3$, неравенство

$$\|t_n\| \geq \sqrt{a_m^2 + b_m^2}.$$

13. Докажите, что среди всех тригонометрических многочленов t_n степени n с данными старшими коэффициентами a_n , b_n наименьшую норму $\|t_n\|$ имеет тригонометрический многочлен $a_n \cos nx + b_n \sin nx$ и только он.

14*. Назовем *нормой* и обозначим $\|p_n\|$ максимум модуля многочлена p_n на отрезке $[-1, 1]$. Докажите, что среди всех многочленов p_n степени n с данным старшим коэффициентом a_n наименьшую норму имеет многочлен Чебышёва $a_n 2^{1-n} T_n(x)$.

15*. а) Для любого $n \in \mathbb{N}$ существует многочлен $P_n(x) \in \mathbb{Z}[x]$ такой, что $2 \cos nt = P_n(2 \cos t)$.

б) Выведите из а), что при любом $q \in \mathbb{Q}$ или $\cos q\pi \in \{0, \pm 1/2, \pm 1\}$, или число $\cos q\pi$ иррационально.

16*. Вычислите $\sum_{k=0}^n q^k \cos(kx + \alpha)$.

17*. Вычислите $\sum_{k=0}^n \cos^2 kx$.

18*. Решите уравнение

$$\cos \varphi + C_n^1 \cos(\varphi + \alpha)x + \dots + C_n^n \cos(\varphi + \alpha n)x^n = 0.$$

19. Докажите тождества и найдите корни тригонометрических многочленов

$$\frac{1}{2} + \cos x + \dots + \cos nx = \frac{\sin \frac{2n+1}{2}x}{2 \sin \frac{x}{2}} \quad (\text{ядро Дирихле});$$

$$\cos x + \dots + \cos nx = \frac{\sin \frac{n}{2}x \cos \frac{n+1}{2}x}{\sin \frac{x}{2}};$$

$$\cos x + \cos 3x + \dots + \cos (2n-1)x = \frac{\sin 2nx}{2 \sin x};$$

$$\sin x + \sin 2x + \dots + \sin nx = \frac{\sin \frac{n}{2}x \sin \frac{n+1}{2}x}{\sin \frac{x}{2}};$$

$$\sin x + \sin 3x + \dots + \sin (2n-1)x = \frac{\sin^2 nx}{\sin x};$$

$$\frac{n+1}{2} + n \cos x + (n-1) \cos 2x + \dots + \cos nx = \frac{1}{2} \left[\frac{\sin \frac{n+1}{2}x}{\sin \frac{x}{2}} \right]^2$$

(ядро Фейера).

20*. Докажите, что тригонометрический многочлен

$$\sum_{k=1}^n (a_k \cos kx + b_k \sin kx)$$

всегда имеет корни.

21*. а) Составьте уравнение с корнями $\operatorname{ctg}^2 \left(\frac{k\pi}{2n+1} \right)$, $1 \leq k \leq n$.

б) Докажите, что

$$\sum_{k=0}^n \operatorname{ctg}^2 \left(\frac{k\pi}{2n+1} \right) = n(2n-1)/3 \quad \text{и} \quad \sum_{k=0}^n \cos^2 \left(\frac{k\pi}{2n+1} \right) = 2n(n+1)/3;$$

в) Выведите из б) и неравенства $\operatorname{ctg} \alpha < \frac{1}{\alpha} < \operatorname{cosec} \alpha$, что

$$\frac{2n(2n-1)}{(2n+1)^2} \frac{\pi^2}{6} < 1 + \frac{1}{2^2} + \dots + \frac{1}{n^2} < \frac{2n(2n+2)}{(2n+1)^2} \frac{\pi^2}{6},$$

откуда следует формула Эйлера

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \lim_{n \rightarrow \infty} \left(1 + \frac{1}{2^2} + \dots + \frac{1}{n^2} \right) = \frac{\pi^2}{6}.$$

22*. (М. Рисс *) Докажите, что для любого неотрицательного тригонометрического многочлена

$$t_n(x) = a_0 + \sum_{k=1}^n (a_k \cos kx + b_k \sin kx)$$

справедливо тождество

$$t_n(x) = |h_n(e^{ix})|^2,$$

где h_n — многочлен n -й степени. Если к тому же t_n четный, то h_n можно подобрать так, чтобы он имел только действительные коэффициенты.

* М. Рисс (Marsel Riesz, 1886–1969) — венгерский математик. Работал в Швеции.

23*. Докажите, что для любого неотрицательного тригонометрического многочлена

$$t_n(x) = a_0 + \sum_{k=1}^n (a_k \cos kx + b_k \sin kx)$$

справедливо неравенство

$$t_n(x) \leq (n+1)a_0,$$

которое обращается в равенство лишь для ядра Фейера.

24*. Пусть $t_n(x)$ — тригонометрический многочлен n -й степени,

$$m = \min_{x \in \mathbb{R}} t_n(x), \quad M = \max_{x \in \mathbb{R}} t_n(x).$$

Докажите, что

$$m + \frac{M-m}{n+1} \leq \frac{1}{2\pi} \int_0^{2\pi} t_n(x) dx = a_0 \leq M - \frac{M-m}{n+1}.$$

25*. Докажите, что

$$\text{а) } \cos nx = A \prod_{k=1}^{2n} \sin \frac{x - \theta_k}{2}, \text{ где } \theta_k = \frac{2k-1}{2n}\pi;$$

$$\text{б) } Q_n^{(m)}(x) = \frac{\cos nx}{2n} (-1)^m \operatorname{ctg} \frac{x - \theta_m}{2} = (-1)^{m+1} \frac{\cos nx \sin \frac{x - (\pi + \theta_m)}{2}}{2n \sin \frac{x - \theta_m}{2}}$$

есть тригонометрический многочлен n -й степени такой, что

$$Q_n^{(m)}(\theta_k) = \begin{cases} 0, & k \neq m; \\ 1, & k = m. \end{cases}$$

26*. Докажите, что для любого тригонометрического многочлена

$$t_n(x) = a_0 + \sum_{k=1}^n (a_k \cos kx + b_k \sin kx)$$

справедливы равенства

$$t_n(x) = a_n \cos nx + \frac{\cos nx}{2n} \sum_{k=1}^{2n} (-1)^k \operatorname{ctg} \frac{x - \theta_k}{2} t_n(\theta_k),$$

$$t'_n(0) = \frac{1}{4n} \sum_{k=1}^{2n} (-1)^{k+1} \frac{1}{\sin^2 \theta_k/2} t_n(\theta_k);$$

формула М. Рисса для производной тригонометрического многочлена

$$t'_n(0) = \frac{1}{4n} \sum_{k=1}^{2n} (-1)^{k+1} \frac{1}{\sin^2 \theta_k/2} t_n(x - \theta_k);$$

неравенство С. Н. Бернштейна *

$$\max_{x \in \mathbb{R}} |t'_n(x)| \leq n \max_{x \in \mathbb{R}} |t_n(x)|.$$

§ 4.18. Расширения полей

Расширение поля путем присоединения корня неприводимого над ним многочлена — это важнейшая и простейшая конструкция теории полей, причем единственная, которую мы будем изучать.

Рассмотрим поле F и кольцо многочленов над ним $F[x]$. Пусть многочлен $f(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$ неприводим над этим полем. Оказывается, можно дополнить поле F новым элементом α таким, что для него выполняется тождество

$$f(\alpha) = a_0\alpha^n + a_1\alpha^{n-1} + \dots + a_{n-1}\alpha + a_n = 0. \quad (*)$$

Операции на множестве формальных выражений («многочленов») вида

$$\varphi(\alpha) = b_0\alpha^m + b_1\alpha^{m-1} + \dots + b_{m-1}\alpha + b_m,$$

где $b_i \in F$, $0 \leq m < n$, определим следующим образом.

Определение 111. *Сложение* определяется так же, как и сложение многочленов (при этом выполняются все аксиомы абелевой группы по сложению), *умножение* определяется как умножение многочленов, но с последующим использованием тождества (*), т. е. после обычного умножения многочленов и деления произведения на $f(\alpha)$ с остатком будем считать *произведением* этот остаток.

Очевидно, степень произведения не превосходит $n - 1$ и операция умножения похожа на умножение в поле вычетов по простому модулю. *Нейтральным элементом* для умножения является 1.

Докажем существование *обратного элемента* по умножению. По условию многочлен $f(x)$ неприводим, поэтому любой не равный нулю

* Бернштейн Сергей Натанович (1880–1968) — советский математик, академик, иностранный член Парижской академии наук.

многочлен $\varphi(x)$ степени, меньшей n , взаимно прост с ним, а значит, можно подобрать такие многочлены $\chi(x)$ и $\mu(x)$, что $f(x)\chi(x) + \mu(x)\varphi(x) = 1$. Подставляя $x = \alpha$, получим $\mu(\alpha)\varphi(\alpha) = 1$.

Упражнение 179. Показать, что для введенных операций выполняются все аксиомы поля.

Определение 112. Построенное поле называется *расширением* поля F с помощью корня многочлена $f(x)$ и обозначается $F(\alpha)$.

Упражнение 180. Пусть F — поле вычетов по модулю 2, многочлен $x^2 + x + 1$ неприводим над этим полем. Обозначим через α корень этого многочлена, тогда $\alpha^2 + \alpha + 1 = 0$. Проверьте, что $F(\alpha)$ состоит из элементов 0, 1, α , $\alpha + 1$ и операции сложения и умножения в этом поле из 4 элементов определяются по следующим таблицам Кэли:

+	0	1	α	$\alpha + 1$
0	0	1	α	$\alpha + 1$
1	1	0	$\alpha + 1$	α
α	α	$\alpha + 1$	0	1
$\alpha + 1$	$\alpha + 1$	α	1	0

·	0	1	α	$\alpha + 1$
0	0	0	0	0
1	0	1	α	$\alpha + 1$
α	0	α	$\alpha + 1$	1
$\alpha + 1$	0	$\alpha + 1$	1	α

Упражнение 181. Проверьте, используя эти таблицы, что выполняются все аксиомы поля.

Упражнение 182. Рассмотрим поле действительных чисел $\mathbb{R}$ и неприводимый над ним многочлен $x^2 + 1$. Обозначим буквой i корень этого многочлена: $i^2 + 1 = 0$. Получите указанным выше способом расширение поля действительных чисел с помощью корня рассматриваемого многочлена $\mathbb{R}[i]$ и проверьте, что это расширение есть не что иное, как поле комплексных чисел.

Определение 113. Множество K комплексных чисел (не обязательно всех) называется *числовым полем*, если для него выполняются условия:

- а) $\alpha, \beta \in K \Rightarrow \alpha \pm \beta \in K$;
- б) $\alpha, \beta \in K \Rightarrow \alpha \cdot \beta \in K$ и (при условии $\beta \neq 0$) $\alpha/\beta \in K$;
- в) поле K содержит не менее двух элементов.

Теорема 113. Всякое числовое поле K содержит все рациональные числа.

Доказательство. Во-первых, поле K содержит 0 и 1. В самом деле, пусть α, β — два различных элемента K , тогда $0 = \alpha - \alpha$ и $1 = \alpha/\alpha$, где α считаем не равным 0.

Во-вторых, поле K содержит все целые числа. Действительно, если $n \in \mathbb{Z}$ и $n > 0$, то $n = \underbrace{1 + \dots + 1}_{n \text{ раз}} \in K$. Если же $n \in \mathbb{Z}$ и $n < 0$, то $-n > 0 \Rightarrow -n \in K$. Но тогда $n = 0 - (-n) \in K$. Осталось заметить, что всякое рациональное число есть частное двух целых $n_1/n_2 \in K$. $\square$

Определение 114. Если поле K_1 содержит поле K_2 , то говорят, что K_1 является *расширением* K_2 .

Примером расширения поля K служит поле, получающееся присоединением к полю K некоторых чисел $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{C}$. Оно обозначается $K(\alpha_1, \alpha_2, \dots, \alpha_n)$. По определению поле $K(\alpha_1, \alpha_2, \dots, \alpha_n)$ есть *наименьшее* из полей, содержащее все числа из поля K и числа $(\alpha_1, \alpha_2, \dots, \alpha_n)$.

Теорема 114. Поле $K(\alpha_1, \alpha_2, \dots, \alpha_n)$ есть множество чисел вида

$$\frac{P(\alpha_1, \alpha_2, \dots, \alpha_n)}{Q(\alpha_1, \alpha_2, \dots, \alpha_n)},$$

где $P(\alpha_1, \alpha_2, \dots, \alpha_n)$, $Q(\alpha_1, \alpha_2, \dots, \alpha_n)$ — многочлены от n переменных с коэффициентами из поля K и $Q(\alpha_1, \alpha_2, \dots, \alpha_n) \neq 0$.

Доказательство. По определению поля $K(\alpha_1, \alpha_2, \dots, \alpha_n)$ оно содержит все числа вида $P(\alpha_1, \alpha_2, \dots, \alpha_n)$ и $Q(\alpha_1, \alpha_2, \dots, \alpha_n)$, а значит, и частные

$$\frac{P(\alpha_1, \alpha_2, \dots, \alpha_n)}{Q(\alpha_1, \alpha_2, \dots, \alpha_n)}.$$

Осталось заметить, что множество таких частных является числовым полем, так как сумма, разность, произведение и частное чисел такого вида тоже является числом вида

$$\frac{F(\alpha_1, \alpha_2, \dots, \alpha_n)}{G(\alpha_1, \alpha_2, \dots, \alpha_n)}$$

для некоторых многочленов $F(\alpha_1, \alpha_2, \dots, \alpha_n)$ и $G(\alpha_1, \alpha_2, \dots, \alpha_n) \neq 0$. $\square$

Примеры. 1. Если $K = \mathbb{C}$, то $K(\alpha_1, \alpha_2, \dots, \alpha_n) = \mathbb{C}$.

2. Если $K = \mathbb{Q}$, $\alpha = \sqrt{2}$, то $\mathbb{Q}(\sqrt{2})$ — *квадратичное расширение* поля $\mathbb{Q}$.

3. Если $K = \mathbb{Q}$, α_i ($i = 1, \dots, n$) — различные корни n -й степени из единицы, то расширение поля рациональных чисел $\mathbb{Q}(\alpha_1, \alpha_2, \dots, \alpha_n)$ называется *полем деления круга на n частей*.

Упражнение 183. Проверьте, что

$$\begin{aligned} K(\alpha_1, \alpha_2, \dots, \alpha_n) &= K(\alpha_1)(\alpha_2, \dots, \alpha_n) = K(\alpha_1, \alpha_2)(\alpha_3, \dots, \alpha_n) = \\ &= K(\alpha_1, \alpha_2, \dots, \alpha_{n-1})(\alpha_n). \end{aligned}$$

Определение 115. *Простым расширением поля K называют поле вида $K(\alpha)$, где $\alpha \in \mathbb{C}$.*

Для простых расширений существенно, является ли α корнем некоторого многочлена $f(x)$ с коэффициентами из поля K или нет.

Определение 116. Число $\alpha \in \mathbb{C}$ называется *алгебраическим* над K , если существует многочлен $f(x) \in K[x]$ такой, что $f(\alpha) = 0$. Алгебраическое над $\mathbb{Q}$ число называется (просто) *алгебраическим* числом.

Напомним, что многочлен f *неприводим* над полем K , если он разлагается в произведение многочленов над K только тривиальным образом, а многочлен с целыми коэффициентами f называется *неприводимым над $\mathbb{Z}$* , если из того, что $f = g \cdot h$ и $g, h \in \mathbb{Z}[x]$, следует, что $(\deg g)(\deg h) = 0$.

Теорема 115. *Пусть K — числовое поле, $f(x)$ — неприводимый над K многочлен. Тогда, если $f_n(\alpha) = 0$, $\alpha \in \mathbb{C}$, то простое расширение $K(\alpha)$ поля K совпадает с множеством*

$$\{a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} : a_0, \dots, a_{n-1} \in K\}.$$

Доказательство. Пусть $\beta = \frac{P(\alpha)}{Q(\alpha)} \in K(\alpha)$ — произвольный элемент этого поля. Представим его в указанном виде.

Заметим сначала, что многочлен $f(x)$ взаимно прост с $Q(x)$. В самом деле, по условию, у многочлена $f(x)$ нет нетривиальных делителей, а если $f(x)$ — делитель $Q(x)$, то $Q(\alpha) = 0$, чего не может быть.

Воспользуемся теперь известным нам линейным представлением НОД, т.е. тождеством $Q(x)u(x) + f(x)v(x) = 1$, где многочлены $u(x), v(x) \in K[x]$. Подставив в него $x = \alpha$, получим, что

$$1 = u(\alpha) \cdot 0 + v(\alpha) \cdot Q(\alpha) = v(\alpha) \cdot Q(\alpha).$$

Значит, $\frac{1}{Q(\alpha)} = v(\alpha)$ и $\frac{P(\alpha)}{Q(\alpha)} = P(\alpha)v(\alpha)$. Поэтому числа из поля $K(\alpha)$ представляются как значения многочленов с коэффициентами из поля K .

Осталось доказать, что для этого можно брать многочлены степени меньших, чем n . Действительно, пусть $\beta = F(\alpha) \in K(\alpha)$. Поделим $F(x)$ на $f(x)$ с остатком и получим равенство

$$F(x) = f(x)q(x) + r(x), \quad \text{где} \quad \deg r(x) < \deg f(x) = n.$$

Подставив в него $x = \alpha$, найдем, что $\beta = F(\alpha) = 0 \cdot q(\alpha) + r(\alpha) = r(\alpha)$. $\square$

Лемма 29 (об аннулирующем многочлене). Пусть $f(x)$ — неприводимый многочлен, $f(\alpha) = q(\alpha) = 0$, тогда $q(x)$ делится на $f(x)$.

Доказательство. Пусть f не делит q , тогда $\text{НОД}(f(x), q(x)) = 1$, значит, согласно лемме о линейном представлении НОД для некоторых многочленов u, v выполняется равенство $1 = fu + qv$. Но тогда, подставляя в это равенство $x = \alpha$, получаем противоречие: $1 = 0$. $\square$

Теорема 116 (об аннулирующем многочлене). Для всякого алгебраического числа α (над полем K) существует единственный неприводимый многочлен $f(x) \in K[x]$ с единичным старшим коэффициентом такой, что $f(\alpha) = 0$.

Доказательство. Существование. Очевидно, существует $g(x) \in K[x]$ такой, что $g(\alpha) = 0$. Согласно теореме 83 этот многочлен однозначно разлагается на неприводимые множители. Число α будет корнем одного из таких множителей.

Единственность. Пусть $f_1(\alpha) = f_2(\alpha) = 0$, многочлены f_1, f_2 неприводимы над K и имеют единичные старшие коэффициенты. Тогда по предыдущей лемме $f_1 \mid f_2$ и $f_2 \mid f_1$, значит, $f_1 = f_2$. $\square$

Задачи и упражнения к § 4.18

1. Докажите, что $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ — поле, в котором многочлен $x^2 - 2$ имеет корень.

2. Докажите, что $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{Q}\}$ — поле, в котором многочлен $x^3 - 2$ имеет корень.

3. Устраните иррациональность в знаменателях дробей

$$\frac{1}{1 + \sqrt[3]{2}}, \quad \frac{\alpha + 1}{\alpha^2 + \alpha + 1},$$

где $\alpha^3 - \alpha - 1 = 0$.

4*. Устраните иррациональность в знаменателе дроби

$$\frac{1}{1 + \sqrt[3]{2} + \sqrt[3]{3}}.$$

5*. Устраните иррациональность в знаменателе дроби

$$\frac{2}{\sqrt{4 - 3\sqrt[4]{5} + 2\sqrt{5} - \sqrt[4]{125}}}.$$

6. Составить уравнение с целыми коэффициентами с корнем $\lambda = \alpha^2 + \alpha + 1$, где $\alpha^3 - \alpha - 1 = 0$.

7. Составить уравнение с целыми коэффициентами с корнем
- а) $\sqrt{2} + \sqrt{3}$; в) $\sqrt[3]{2} + \sqrt[3]{3}$;
 б) $\sqrt{2} + \sqrt{3} + \sqrt{5}$; г) $\sqrt[3]{2} + \sqrt[3]{3} + \sqrt[3]{5}$.
8. Докажите иррациональность чисел
- а) $\sqrt{2} + \sqrt{3}$; в) $\sqrt[3]{2} + \sqrt[3]{3}$;
 б) $\sqrt{2} + \sqrt{3} + \sqrt{5}$; г) $\sqrt[3]{2} + \sqrt[3]{3} + \sqrt[3]{5}$.
9. Построить расширение поля $\mathbb{Z}_3$ с помощью многочлена $x^2 + 1$.
10. Докажите существование полей порядка p^2 и p^3 .
- 11*. Пусть в некотором поле F характеристики p многочлен $x^{p^m} - x$ раскладывается на линейные множители. Докажите, что все корни этого многочлена различны и образуют поле порядка p^m .
- 12*. Докажите, что $x^{p^m} - x$ делит $x^{p^n} - x$ тогда и только тогда, когда m делит n .
- 13*. Пусть F — конечное поле порядка p^n . Докажите, что все элементы поля F , удовлетворяющие уравнению $x^{p^m} - x = 0$, где m — делитель n , образуют подполе порядка p^m , причем подполе такого порядка единственно.
- 14*. Докажите, что любое подполе поля порядка p^n имеет порядок p^m , где m — делитель n .
- 15*. Пусть $f(x)$ — неприводимый многочлен степени m над полем $\mathbb{Z}_p$. Докажите, что $f(x)$ делит $x^{p^m} - x$.
- 16**. Обозначим через $f_m(x)$ произведение всех неприводимых многочленов степени m над полем $\mathbb{Z}_p$. Докажите, что
- $$x^{p^n} - x = \prod_{d|n} f_d(x).$$
- 17*. Найдите $f_m(x)$ при простом n .
- 18*. Найдите $f_m(x)$ при $p = 2$ и $n = 4, 6, 8$.
- 19*. Найдите $f_m(x)$ при любом m .
- 20**. Докажите существование полей порядка p^n .
- 21*. Число $\alpha \in C$ называется *алгебраическим*, если является корнем многочлена с целыми коэффициентами, и *целым алгебраическим*, если старший коэффициент этого многочлена равен единице. Докажите, что алгебраические числа образуют поле, а целые алгебраические — кольцо в нем.
- 22*. *Сопряженными* к алгебраическому числу называются корни многочлена с целыми коэффициентами минимальной степени, аннулирующего это число. Произведение этого числа на все сопряженные к нему называется его *нормой*. Докажите, что норма алгебраического числа — рациональное, а норма целого алгебраического числа — целое число.
- 23*. Докажите, что любой многочлен с алгебраическими коэффициентами имеет только алгебраические корни.

Дополнительные задачи о многочленах

1*. Любой многочлен из $\mathbb{C}[x]$ при любом $n \in \mathbb{N}$ можно представить в виде суммы n -х степеней многочленов из $\mathbb{C}[x]$.

2*. (Обобщенная теорема Ролля.) Если многочлен $f(x) \in \mathbb{R}[x]$ имеет на отрезке $[a, b]$ n действительных корней с учетом кратности, то при любом $k < n$ производная k -го порядка от $f(x)$ на этом отрезке имеет не менее $n - k$ корней с учетом кратности.

3. (Ролль *.) Если все корни многочлена $f(x) \in \mathbb{R}[x]$ действительны, то при любом $k < n$ производная k -го порядка от $f(x)$ имеет только действительные корни.

4*. Если все корни многочлена $f(x) \in \mathbb{R}[x]$ действительны, то при $\lambda \in \mathbb{R}$ все корни $f(x) + \lambda f'(x)$ также действительны.

У к а з а н и е. Рассмотреть $e^{\lambda x} f(x)$ и применить теорему Ролля.

5*. Если все корни $f(x), g(x) \in \mathbb{R}[x]$ действительны, $g(x) = a_n x^n + \dots + a_0$, то у многочлена $F(x) = a_n f(x)^{(n)} + \dots + a_0 f(x)$ все корни также действительны.

У к а з а н и е. Заметить, что $g(x) = a_n \prod_i (x - \alpha_i)$, рассмотреть последовательность $F_0(x) = a_n f(x)$, $F_k(x) = F_{k-1}(x) + \lambda_k F'_k(x)$, $F_n(x) = F(x)$ и применить предыдущую задачу.

6*. Если все корни многочленов $f(x), g(x) \in \mathbb{R}[x]$ действительные, некрatные и разделяются, т. е. между соседними корнями одного всегда лежит корень другого, то при любых a и $b \in \mathbb{R}$ у многочлена $ag(x) + bf(x)$ все корни действительны.

7. Если многочлен $f(x) \in \mathbb{R}[x]$ имеет кратный корень, то при достаточно малом t либо $f(x) + t$, либо $f(x) - t$ имеет недействительные корни.

8*. Если многочлены $f(x), g(x) \in \mathbb{R}[x]$ взаимно просты, и при любых a и $b \in \mathbb{R}$ у многочлена $ag(x) + bf(x)$ все корни действительны, то все корни многочленов $f(x), g(x) \in \mathbb{R}[x]$ действительные, некрatные и разделяются.

9*. Если все корни многочленов $f(x), g(x) \in \mathbb{R}[x]$ действительные, некрatные и разделяются, то корни их производных действительны, некрatны и разделяются.

10*. Если все корни многочленов $f(x) - a, f(x) - b \in \mathbb{R}[x]$, $a, b \in \mathbb{R}$, действительные, $a < c < b$, то все корни многочлена $f(x) - c$ действительные.

* М. Ролль (Michel Rolle, 1652–1719) — французский математик, бывший противником дифференциального и интегрального исчисления.

11*. Определить число действительных корней многочленов

$$x^{2n_1+1} + \dots + x^{2n_k+1} + a, \quad nx^n - x^{n-1} - x^{n-2} - \dots - 1,$$

$$\frac{x^n}{n} + \frac{x^{n-1}}{n-1} + \dots + \frac{x^2}{2} + x + 1.$$

12. Докажите, что многочлен

$$a_{2n}x^{2n} + a_{2n-2}x^{2n-2} + \dots + a_2x^2 + a_1x + a_0$$

имеет не более двух действительных корней, если $a_k \geq 0$ при $k > 1$.

13*. (Маклорен *.) Если коэффициенты у $f(x)$ неотрицательны, то все действительные корни не больше 0.

14*. (Маклорен.) Если несколько старших коэффициентов неотрицательны, а последние $m+1$ отрицательны, то все действительные корни многочлена

$$g(x) = a_nx^n + \dots + a_0$$

не превосходят

а) $\rho + \max_{a_k < 0} {}^{n-m}\sqrt{|a_k/a_n \rho^{m-k}|}$ при любом $\rho > 0$,

б) $2 \max_{a_k < 0} {}^{n-k}\sqrt{|a_k/a_n|}$,

в) ${}^{n-m}\sqrt{|a_m/a_n|} + {}^{m-k}\sqrt{|a_k/a_m|}$.

15*. (Оценки Маклорена.) Корни произвольного многочлена

$$g(x) = a_nx^n + \dots + a_0 \in \mathbb{C}[x]$$

по модулю не превосходят

а) $1 + \max_{k < n} |a_k/a_n|$; в) $2 \max_{k < n} {}^{n-k}\sqrt{|a_k/a_n|}$;

б) $\rho + \max_{k < n} |a_k/a_n \rho^{n-k-1}|$; г) $|a_{n-1}/a_n| + \max_{k < n} {}^{n-k-1}\sqrt{|a_k/a_{n-1}|}$.

16*. (Ньютон.) Если $f(x) \in \mathbb{R}[x]$, $f(a) \geq 0$, $f'(a) \geq 0$, ..., $f^{(n)}(a) \geq 0$, $\deg f(x) = n$, то все действительные корни многочлена $f(x)$ не превосходят a .

17*. Многочлен $x^n - p_1x^{n-1} - \dots - p_n$ при $p_i \geq 0$, $p_1 + \dots + p_n > 0$, имеет единственный положительный корень.

18. Любой корень многочлена $z^n + a_1z^{n-1} + \dots + a_n \in \mathbb{C}[z]$ не превосходит по модулю единственного положительного корня многочлена

$$x^n - |a_1|x^{n-1} - \dots - |a_n|.$$

* Маклорен (Colin Maclaurin, 1698–1746) — шотландский математик.

19. Пусть $p_0 > p_1 > \dots > p_n > 0$. Докажите, что внутри круга $|z| \leq 1$ нет нулей многочлена $p_0 + p_1 z + \dots + p_n z^n$.

20. Пусть $p_0 > p_1 > \dots > p_n > 0$, $\alpha = \min(p_1/p_0, p_2/p_1, \dots, p_n/p_{n-1})$. Докажите, что многочлен $p_0 z^n + p_1 z^{n-1} + \dots + p_n$ не имеет нулей в круге $|z| \leq \alpha$.

21*. Пусть $p_0 \geq p_1 \geq \dots \geq p_n \geq 0$, $f(z) = p_0 z^n + p_1 z^{n-1} + \dots + p_n$, $f(\lambda) = 0$, $|\lambda| \geq 1$. Докажите, что λ есть некоторый корень из 1.

22*. Если многочлен

$$f(x, y) = a_n x^n + a_{n-1} x^{n-1} y + \dots + a_1 x y^{n-1} + a_0 y^n \in \mathbb{R}[x, y]$$

разлагается на линейные множители, то это же верно для $\frac{\partial f}{\partial x}$ и $\frac{\partial f}{\partial y}$.
У к а з а н и е. Рассмотреть многочлены

$$g(x) = a_n x^n + \dots + a_0 \quad \text{и} \quad h(x) = a_0 x^n + \dots + a_n$$

и применить теорему Ролля.

23. Если трехчлен

$$f(x, y) = ax^2 + bxy + cy^2 \in \mathbb{R}[x, y]$$

разлагается на линейные множители, то $b^2 \geq ac$, и обратно.

24*. Пусть $a_1, \dots, a_n > 0$, $\sigma_k = \sum a_{i_1} a_{i_2} \dots a_{i_k}$ — элементарный симметрический многочлен от переменных a_i , $p_k = \sigma_k / C_n^k$. Тогда $p_k^2 \geq p_{k-1} p_{k+1}$ при $2 \leq k \leq n-1$.

У к а з а н и е. Рассмотреть многочлен $f(x, y) = \prod_{k=1}^n (x - a_k y)$, его производную $\frac{\partial^{n-2} f}{\partial^{k-1} x \partial^{n-1-k} y}$ и применить предыдущую задачу.

25*. (Неравенства Ньютона—Маклорена.) Докажите, что в обозначениях предыдущей задачи

$$p_1 \geq p_2^{1/2} \geq \dots \geq p_n^{1/n}.$$

У к а з а н и е. Перемножить неравенства $p_k^{2k} \geq p_{k-1}^k p_{k+1}^k$.

26*. (Оценка Цассенхауза.) Корни произвольного многочлена

$$g(x) = x^n + a_{n-1} x^{n-1} + \dots + a_0 \in \mathbb{C}[x]$$

по модулю не превосходят

$$\text{а) } \max_{k < n} \frac{1}{2^{1/n} - 1} n^{-k} \sqrt[n]{\frac{|a_k|}{C_n^k}}; \quad \text{б) } 2 \max_{k < n} n^{-k} \sqrt[n]{|a_k|}.$$

Дополнительные задачи о комплексных числах

1*. а) Докажите, что множество G всех комплексных чисел с целыми действительными и мнимыми частями является целостным кольцом (*кольцом гауссовых целых чисел*).

б) Пусть ω — гауссово число. Докажите, что

$$\omega \in \mathbb{Z} \iff |\omega| = \pm\omega,$$

$$\omega \text{ обратимо в кольце } G \iff |\omega| = 1 \iff \omega \in \{\pm 1, \pm i\}.$$

в) Пусть ω — гауссово число, $|\omega| = \sqrt{p}$, p — простое число. Тогда ω — (*простой*) элемент в G (*простое гауссово число*).

2. Множество всех гауссовых чисел, кратных в G данному числу ω , изображается на комплексной плоскости квадратной решеткой.

3. Для любых ω и $z \in G$, $z \neq 0$, найдутся u и $v \in G$ такие, что

$$\omega = zu + v, \quad |v| \leq |z|$$

(*деление с остатком*).

4*. Если простой элемент ω делит произведение z и u в G , то он делит либо z , либо u .

5. Докажите, что для кольца целых гауссовых чисел справедлива теорема об однозначном разложении на простые множители.

6*. С точностью до умножения на $\pm 1, \pm i$ все простые элементы в G исчерпываются следующими: 1, обычные простые вида $4k + 3$ и числа вида $x + yi$, где x — четно, y — нечетно и $x^2 + y^2$ — обычное простое.

7*. Подобно определению кольца вычетов $\mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p$ определите кольцо G_p и докажите, что оно будет полем порядка p^2 при простом $p = 4k + 3$ и не будет полем при простом $p = 4k + 1$. У к а з а н и е. При $p = 4k + 1$ выполняется $((2k!)^2 + 1) \bmod p = 0$.

8*. Докажите, что простое вида $4k + 1$ представимо в виде суммы квадратов двух целых чисел.

9*. Докажите, что любое натуральное n представимо в виде суммы квадратов двух целых чисел тогда и только тогда, когда простые вида $4k + 3$ входят в его разложение в четных степенях.

10*. Решите в целых числах уравнение

$$x^2 + y^2 = z^n, \quad n > 1.$$

У к а з а н и е. $x^2 + y^2 = (x + yi)(x - yi)$.

11*. Решите в целых числах уравнение

$$x^2 + 4 = z^3.$$

12*. Докажите, что при простом p , $p > 2$,

$$(1 - i)^p \equiv 1 - i^p \pmod{p},$$

и, используя равенство $(1 - i)^2 = -2i$, докажите, что

$$2^{(p-1)/2} \equiv \frac{1 - i^p}{1 - i} \pmod{p}.$$

13*. Докажите, что при простом p , $p > 2$, символ Лежандра $\left(\frac{2}{p}\right)$ равен $(-1)^{\frac{p^2-1}{8}}$. Вычислите символ Лежандра $\left(\frac{-2}{p}\right)$.

14*. Докажите, что простых вида $8n - 1$ бесконечно много и простых вида $8n + 3$ также бесконечно много.

§ 4.19. Построения циркулем и линейкой

Под построением мы будем понимать выполнение последовательности следующих операций:

- 1) проведение прямой через две заданные точки;
- 2) построение окружности заданного радиуса и с заданным центром.

При этом считается, что с самого начала нам задан единичный отрезок. Откладывая его последовательно, мы получим отрезок, равный заданному натуральному числу. Заметим, что мы можем построить отрезок, длина которого равна отношению длин двух заданных отрезков. Поэтому можно считать, что с самого начала нам даны все отрезки, длины которых являются положительными рациональными числами.

Задача на построение есть задача, в которой требуется построить, отправляясь от заданных отрезков, некоторый новый отрезок. Многие задачи на построение геометрических образов сводятся к таким задачам. Например, рассмотрим три классические задачи древности.

1. Построить куб, имеющий объем в два раза больше, чем заданный куб. Будем считать сторону заданного куба единичным отрезком. Тогда задача сводится к построению отрезка, имеющего длину $\sqrt[3]{2}$.

2. По заданному углу α построить угол величины $\alpha/3$. Очевидно, эту задачу можно свести к построению отрезка $\cos \alpha/3$, при условии, что, кроме единичного отрезка, задан отрезок длины $\cos \alpha$.

3. Построить правильный семиугольник, вписанный в окружность с радиусом единичной длины. Очевидно, достаточно построить угол величины $\frac{2\pi}{7}$ или отрезок длины $\cos \frac{2\pi}{7}$.

Для того, чтобы попытаться решить эти проблемы или доказать их неразрешимость, сведем задачу построения отрезков к алгебраическим задачам.

Прежде всего заметим, что если мы построили отрезок длины a , то можем построить любой отрезок, длина которого представляет собой любое положительное число из поля $\mathbb{Q}(a)$. В самом деле, по заданным отрезкам x и y можно построить $x \pm y$, $x \cdot y$, x/y . Будем тогда говорить, что мы можем построить поле $\mathbb{Q}(a)$.

Известно из курса геометрии, что посредством циркуля и линейки по отрезку a можно построить отрезок $\sqrt{a}$ при условии, если задан единственный отрезок. Для этого строим окружность диаметром $a + 1$ и восстановим перпендикуляр к диаметру на расстоянии 1 от его конца.

Таким образом, мы можем строить и квадратичные расширения $\mathbb{Q}(\sqrt{a})$.

Определение 117. Назовем последовательность расширений

$$K_0 \subset K_1 \subset K_2 \dots \subset K_n$$

пифагоровым расширением, если $K_0 = \mathbb{Q}$ и $K_s = K_{s-1}(\sqrt{a_s})$, где $a_s \in K_{s-1}$, $\sqrt{a_s} \notin K_{s-1}$, $a_s > 0$. Поле K_n в этом случае станем также называть пифагоровым расширением. Числа, принадлежащие пифагорову расширению, будем называть *пифагоровыми числами*.

Теорема 117 (о пифагоровых числах). *Число a можно построить тогда и только тогда, когда оно является пифагоровым.*

Доказательство. Достаточность мы уже доказали: мы умеем производить четыре арифметические операции и извлекать квадратный корень при помощи циркуля и линейки.

Докажем необходимость. Для этого воспользуемся координатным методом. Проведем прямую и ей перпендикулярную прямую (т. е. построим систему координат). На этих прямых мы можем отложить любую рациональную точку, так что с самого начала мы можем считать заданными точки плоскости, имеющие рациональные координаты. При наших построениях мы можем рассматривать абсциссы и ординаты вновь построенных точек — ведь это тоже «построенные отрезки».

Новые точки получаются только следующим образом:

- (i) как пересечение двух построенных прямых;
- (ii) как пересечение построенной прямой и построенной окружности;
- (iii) как пересечение двух построенных окружностей;
- (iv) произвольно выбранные точки.

Поэтому координаты этих точек получаются как решения следующих систем уравнений с уже построенными коэффициентами:

$$\begin{cases} a_1x + b_1y + c_1 = 0; \\ a_2x + b_2y + c_2 = 0; \end{cases} \quad (\text{I})$$

$$\begin{cases} a_1x + b_1y + c_1 = 0; \\ x^2 + y^2 + a_2x + b_2y + c_2 = 0; \end{cases} \quad (\text{II})$$

$$\begin{cases} x^2 + y^2 + a_1x + b_1y + c_1 = 0; \\ x^2 + y^2 + a_2x + b_2y + c_2 = 0. \end{cases} \quad (\text{III})$$

Мы считаем очевидным утверждение о том, что у уравнений построенных прямых и окружностей коэффициенты тоже можно считать построенными (проверьте это сами).

Докажем нашу теорему индукцией по числу элементарных операций, на которые раскладывается любое построение. С самого начала заданы рациональные числа, т. е. числа из поля $\mathbb{Q} = K_0$. Элементарное построение — это добавление координат точки, получающейся операциями (i), (ii), (iii), к построенным числам. Однако, как видно из уравнений для этих координат, они (эти координаты) получаются из коэффициентов (т. е. из уже построенных чисел) при помощи четырех операций арифметики и извлечения корня. Решение системы (II) сводится к нахождению корней квадратного уравнения (из первого уравнения системы выразим одну координату через другую и подставим во второе уравнение). Решение системы (III) эквивалентно решению системы

$$\begin{cases} x^2 + y^2 + a_1x + b_1y + c_1 = 0; \\ (a_1 - a_2)x + (b_1 - b_2)y + (c_1 - c_2) = 0. \end{cases} \quad \square$$

Теорема 118. *Если кубический многочлен с рациональными коэффициентами не имеет рациональных корней, то нельзя построить ни одного из его корней.*

Доказательство. Рассуждаем от противного. Пусть x_1, x_2, x_3 — корни многочлена $f(x)$ и существует пифагорово расширение $\mathbb{Q} = K_0 \subset K_1 \subset \dots \subset K_n$ такое, что $x_1 \in K_n$, $x_1, x_2, x_3 \notin K_{n-1}$. Тогда число x_1 имеет вид $x_1 = a + b\sqrt{d}$, где $a, b, d \in K_{n-1}$, $\sqrt{d} \notin K_{n-1}$, $b \neq 0$.

Заметим, что $\bar{x}_1 = a - b\sqrt{d} \in K_n$ — тоже корень $f(x)$. В самом деле, операция сопряжения в квадратичном расширении $K_{n-1} \subset K_n$ имеет вид $\overline{a + b\sqrt{d}} = a - b\sqrt{d}$. Выполняются следующие свойства этой операции:

$$\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2 \quad \text{и} \quad \overline{z_1 z_2} = \bar{z}_1 \bar{z}_2.$$

Применяя многократно эти тождества, можно проверить, что $\overline{f(z)} = f(\bar{z})$ для $z \in K_n$. Значит, для корня $x_1 \in K_n$

$$f(\bar{x}_1) = \overline{f(x_1)} = \bar{0} = 0,$$

поэтому $\bar{x}_1$ — тоже корень многочлена $f(x)$. Пусть $\bar{x}_1 = x_2$. Тогда $x_3 = -b_1 - x_1 - x_2$, где $f(x) = x^3 + b_1x^2 + b_2x + b_3$, $b_i \in \mathbb{Q}$. Значит, $x_3 = -b_1 - 2a \in K_{n-1}$. Противоречие. $\square$

Упражнения

1. Дайте геометрические построения для чисел

$$\sqrt{2}, \quad \sqrt{2 + \sqrt{2}}, \quad \sqrt{2 + \sqrt{2 + \sqrt{2}}}.$$

2. Проверьте правильность следующего построения корней квадратного уравнения $ax^2 + bx + c = 0$: возьмем единичный отрезок AB , проведем $BC = -b/a$ перпендикулярно к AB и $CD = c/a$ перпендикулярно к BC в направлении BA , на диаметре AD построим окружность, пересекающую BC в точках X, Y . Тогда BX и BY — корни уравнения.

3*. Докажите, что корни кубического уравнения с рациональными коэффициентами являются пифагоровыми числами тогда и только тогда, когда оно имеет рациональный корень.

4*. Докажите, что корни уравнения четвертой степени с рациональными коэффициентами являются пифагоровыми числами тогда и только тогда, когда его кубическая резольвента имеет рациональный корень. Кубической резольвентой уравнения

$$x^4 + ax^2 + bx + c = 0$$

является уравнение

$$z^3 + 2az^2 + (a^2 - 4c)z - b^2 = 0.$$

5*. Докажите неразрешимость циркулем и линейкой следующих задач на построение:

- построить треугольник по трем данным биссектрисам;
- построить треугольник по двум биссектрисам и высоте;
- построить треугольник по двум биссектрисам и медиане, выходящей из трех разных вершин;
- построить квадрат, у которого две соседние вершины лежат на одной данной окружности, а две другие — на другой данной окружности.

Введем понятие сложности построения циркулем и линейкой. Допустим, что на плоскости дано некоторое множество точек, прямых и окружностей, которое обозначим M_0 .

Определение 118. Назовем *построением циркулем и линейкой* при заданном M_0 любую последовательность множеств $M_0, M_1, \dots, M_L$, начинающуюся с M_0 и такую, что каждое следующее множество M_{i+1} получается из предыдущего множества M_i добавлением либо некоторой прямой, проходящей через какие-то две точки из множества M_i , либо окружности с центром в какой-то из точек множества M_i и радиусом, равным длине некоторого отрезка с концами в точках из M_i , а также всех точек пересечения добавленной линии со всеми линиями из множества M_i . Число L назовем *сложностью* этого построения. *Сложностью построения* множества M точек, отрезков, окружностей и прямых при заданном M_0 назовем *минимальную* сложность такого построения $M_0, M_1, \dots, M_L$, для которого множество M_L содержит все прямые и окружности из M , все точки из M и концы всех отрезков из M .

Аналогично определяется сложность построения одним циркулем.

Следующие несколько задач принадлежат итальянскому математику Маскерони*.

Задачи Маскерони

1. Дана единичная окружность с диаметром и отрезок длины x , $x < 1$. Постройте на этом диаметре отрезок длины x^2 одним циркулем со сложностью 2.

2. Решите предыдущую задачу со сложностью 3, если диаметр задан только одним своим концом, а не начерчен целиком.

3. Дана единичная окружность и отрезок длины $x > 1$ с началом в ее центре. Постройте отрезок длины x^{-1} одним циркулем со сложностью 2. Постройте отрезок длины x^{-1} одним циркулем со сложностью 3, если отрезок длины x задан только своими концами, а не начерчен целиком.

4. Даны отрезки с длинами a, b, c , где $b, c < 2a$. Постройте одним циркулем со сложностью 3 отрезок длины x такой, что $a : b = c : x$.

5. Даны единичная окружность, отрезок длины $c < 2$ с началом в ее центре и еще отрезок длины $b < 1$. Постройте одним циркулем со сложностью 2 отрезок длины bc .

6. Постройте одним циркулем со сложностью 3 одновременно отрезки длины 2 и 3, лежащие на одной прямой с данным единичным отрезком.

* Л. Маскерони (Lorenzo Mascheroni, 1750–1800). Свою книгу «Геометрия циркуля» он посвятил Наполеону.

7. Поделите пополам отрезок одним циркулем:
 - а) со сложностью 4, если дана прямая, на которой лежит отрезок,
 - б) со сложностью 5, если дан только сам отрезок,
 - в) со сложностью 6, если даны только его концы.
 8. Поделите на три равные части отрезок одним циркулем:
 - а) со сложностью 5, если дана прямая, на которой лежит отрезок,
 - б) со сложностью 8, если дан только сам отрезок,
 - в) со сложностью 11, если даны только его концы.
 9. Разделите циркулем и линейкой отрезок пополам со сложностью 3 и на четыре равные части со сложностью 6.
 10. Разделите циркулем и линейкой отрезок на шесть равных частей со сложностью 8.
 11. Проведите через точку вне прямой параллельную ей прямую со сложностью 3.
 12. На сторонах угла отложены от его вершины отрезки длины a , b и 1 (два из них — на одной стороне, а один — на другой). Постройте со сложностью 3 отрезок длины ab на одной из сторон угла.
- Следующий цикл задач принадлежит датскому математику Мору*.

Задачи Мора

1. Постройте со сложностью 5 одним циркулем одновременно отрезки длины $\sqrt{a^2 - b^2}$, $2\sqrt{a^2 - b^2}$, $2b$, $3b$, $\sqrt{3}b$, если отрезки a и b , $a > b$, заданы.
2. Постройте со сложностью 5 одним циркулем одновременно отрезки длины $\sqrt{2}a$, $\sqrt{3}a$, $\sqrt{8}a$, $2a$, $3a$, если отрезок длины a задан.
3. Постройте со сложностью 11 одним циркулем одновременно отрезки длины $\sqrt{a^2 + b^2}$, $2\sqrt{a^2 + b^2}$, $\sqrt{a^2 - b^2}$, $2\sqrt{a^2 - b^2}$, $\sqrt{2}a$, $\sqrt{3}a$, $\sqrt{8}a$, $2a$, $3a$, $2b$, $3b$, $\sqrt{3}b$, если отрезки a и b , $a > b$, заданы.
4. Постройте со сложностью 15 одним циркулем одновременно отрезки длины $a + b$, $a - b$, $ab/\sqrt{a^2 + b^2}$, $\sqrt{a^2 + b^2}$, $2\sqrt{a^2 + b^2}$, $\sqrt{a^2 - b^2}$, $2\sqrt{a^2 - b^2}$, $\sqrt{2}a$, $\sqrt{3}a$, $\sqrt{8}a$, $2a$, $3a$, $2b$, $3b$, $\sqrt{3}b$, если отрезки a и b , $a > b$, заданы.
5. Если отрезки длины a и b заданы на одной прямой, то отрезок длины $a + b$ можно построить одним циркулем со сложностью 2.
6. Даны отрезки длины 1 и $a < 1$ с общим концом, вложенные один в другой. Постройте со сложностью 7 одним циркулем отрезок длины $\sqrt{a}$.

* Г. Мор (George Mohr, 1640–1697). В написанной им книге «Датский Евклид» он на столетие раньше Маскерони доказал возможность проведения всех геометрических построений одним лишь циркулем.

В случае $a > 1$ подобное построение можно осуществить со сложностью 9.

7.** Докажите теорему Мора—Маскерони о построениях одним циркулем: любое построение, выполнимое циркулем и линейкой, может быть выполнено и одним циркулем.

§ 4.20. Теорема Абеля—Руффини

Теорема 119. *Общее уравнение степени выше пятой неразрешимо в радикалах, т. е. не существует формулы, выражающей его корни через коэффициенты, в которой бы кроме четырех арифметических операций использовалось бы только извлечение комплексных корней произвольных степеней.*

Доказательство. Прежде всего заметим, что теорему достаточно доказать для общего уравнения пятой степени. В самом деле, если бы имелась общая формула для решения уравнения n -й степени, то она бы давала решение в радикалах и для уравнения:

$$x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + a_{n-3}x^{n-3} + a_{n-4}x^{n-4} + a_{n-5}x^{n-5} = 0.$$

Предположим, что общее уравнение пятой степени

$$x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = 0$$

имеет решение в радикалах. Для того чтобы дать удобную для наших целей переформулировку, введем понятие *радикального расширения* $K(\sqrt[n]{a})$ поля K ($a \in K$).

Обозначим через $K(\sqrt[n]{a})$ множество всех выражений вида $f(\sqrt[n]{a})$, где f — рациональная функция с коэффициентами из поля K , а элемент $\sqrt[n]{a}$ удовлетворяет соотношению $(\sqrt[n]{a})^n = a$.

Если поле K — поле всех рациональных функций, то с элементом $\sqrt[n]{a}$ поля $K(\sqrt[n]{a})$ тоже можно связать некоторую функцию. Однако строгое обоснование этого приводит к понятию римановой поверхности, которое не является элементарным. Мы будем выбирать одно значение корня $\sqrt[n]{a}$ и не вдаваться в технические детали. Отметим, что формула, доставляющая решения уравнения, лежит в поле функций, которое получается радикальными расширениями из поля рациональных функций.

Рассмотрим некоторые примеры.

Для общего уравнения второй степени $x^2 + a_1x + a_0 = 0$ формула для решений лежит в поле $K(\sqrt{a_1^2 - 4a_0})$, которое совпадает с полем всех рациональных функций от переменных x_1 и x_2 , для которых $x_1 + x_2 = -a_1$, $x_1x_2 = a_0$.

В общем случае, формула для решения уравнения n -й степени доставляла бы последовательность радикальных расширений, которая бы началась с поля $K_0 = \mathbb{C}(a_0, a_1, \dots, a_4)$ всех рациональных функций, а заканчивалась бы полем всех рациональных функций $K_n = \mathbb{C}(x_1, x_2, x_3, x_4, x_5)$ или некоторым его расширением.

$$K_0 \subset K_1 \subset K_2 \subset \dots \subset K_n.$$

При этом поле K_0 выделялось бы в K_n как множество всех симметрических рациональных функций, т. к. по теореме Виета $a_i = -\sigma_i(x_1, x_2, x_3, x_4, x_5)$, $0 \leq i \leq 4$, а всякая симметрическая рациональная функция выражается через элементарные симметрические функции как рациональная дробь от них.

Интересен вопрос: можем ли мы прийти к некоторому расширению поля $\mathbb{C}(x_1, x_2, x_3, x_4, x_5)$ при последовательном радикальном расширении поля K_0 по формулам, выражающим x_i через $a_0, \dots, a_4$? Ответ на этот вопрос отрицательный. Мы дадим здесь только эскиз доказательства. Рассмотрим вначале пример расширения, соответствующего формулам Кардано. Пусть дано общее уравнение третьей степени

$$x^3 + a_2x^2 + a_1x + a_0 = 0.$$

Замена переменных $x \rightarrow x + a_2/3$ приводит его к виду $x^3 + ax + b = 0$.

Тогда резольвенты Лагранжа $\rho_1 = x_1 + \varepsilon x_2 + \varepsilon^2 x_3$ и $\rho_2 = x_1 + \varepsilon^2 x_2 + \varepsilon x_3$, где $\varepsilon = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$, удовлетворяют условиям:

$$\begin{aligned} \rho_1 \cdot \rho_2 &= x_1^2 + x_2^2 + x_3^2 - x_1x_2 - x_2x_3 - x_3x_1 = \\ &= (x_1 + x_2 + x_3)^2 - 3(x_1x_2 + x_2x_3 + x_3x_1) = -3a, \end{aligned}$$

$$\begin{aligned} \rho_1^3 + \rho_2^3 &= (\rho_1 + \rho_2)[(\rho_1 + \rho_2)^2 - 3\rho_1\rho_2] = 3x_1[9x_1^2 + 9a] = \\ &= 27(x_1^3 + ax_1) = -27b, \end{aligned}$$

$$\begin{aligned} \rho_1^3 - \rho_2^3 &= (\rho_1 - \rho_2)(\rho_1^2 + \rho_1\rho_2 + \rho_2^2) = \\ &= \sqrt{3}(x_2 - x_3)(x_1^2 + \varepsilon^2 x_2^2 + \varepsilon x_3^2 + x_1^2 + \varepsilon x_2^2 + \varepsilon^2 x_3^2 + 2\varepsilon x_1x_2 + \varepsilon^2 x_1x_3 + \\ &+ 2x_2x_3 + 2\varepsilon^2 x_1x_2 + 2\varepsilon x_1x_3 + 2x_2x_3 + x_1^2 + x_2^2 + x_3^2 - x_1x_2 - x_2x_3 - x_3x_1) = \\ &= i\sqrt{3}(x_2 - x_3)(3x_1^2 - 3x_1x_2 - 3x_1x_3 + 3x_2x_3) = \\ &= i\sqrt{27}(x_1 - x_3)(x_2 - x_3)(x_1 - x_2). \end{aligned}$$

Поэтому

$$(\rho_1^3 - \rho_2^3)^2 = -27(x_1 - x_2)^2(x_2 - x_3)^2(x_3 - x_1)^2 = 27(4a^3 + 27b^2).$$

Значит, можно выбрать следующую цепочку радикальных расширений:

$$K_0 \subset K_0(\sqrt{4a^3 + 27b^2}) \subset K_0\left(\sqrt[3]{-\frac{b}{2} + \sqrt{\frac{a^3}{27} + \frac{b^2}{4}}}\right).$$

Заметим, что последнее поле совпадает с полем $\mathbb{C}(x_1, x_2, x_3)$.

Аналогично можно поступить и с уравнением четвертой степени.

Пусть удалось проделать аналогичные выкладки и для общего уравнения пятой степени, и имеется цепочка радикальных расширений:

$$\mathbb{C}(a_0, a_1, a_2, a_3, a_4) = K_0 \subset K_1 \subset \dots \subset K_n = \mathbb{C}(x_1, x_2, x_3, x_4, x_5).$$

Лемма 30. *Справедливо равенство $K_1 = K_0(\sqrt{D})$, где*

$$D = (x_1 - x_2)^2(x_1 - x_3)^2 \dots (x_4 - x_5)^2$$

— дискриминант уравнения пятой степени.

Доказательство. Пусть $K_1 = K_0(\sqrt[r]{a})$ и $a \in K_0$, $r \geq 2$ и

$$\sqrt[r]{a} = f(x_1, x_2, x_3, x_4, x_5) \in \mathbb{C}(x_1, x_2, x_3, x_4, x_5).$$

Тогда для всякой перестановки $\alpha \in S_5$ имеет место равенство $\alpha f = \varepsilon_\alpha f$, где $\varepsilon_\alpha \in \sqrt[r]{a}$, а αf — функция f с переставленными в соответствии с перестановкой α переменными.

Действительно, $(\alpha f)^r = \alpha(f^r) = \alpha a = a = f^r$, так как $a \in \mathbb{C}(\sigma_0, \sigma_1, \dots, \sigma_4)$ (мы воспользовались свойством перестановки переменных $\alpha(h_1 \cdot h_2) = \alpha h_1 \cdot \alpha h_2$). Кроме того, для любой функции h выполняется свойство $\alpha\beta(h) = \alpha(\beta h)$, из которого вытекает тождество $\varepsilon_{\alpha\beta} = \varepsilon_\alpha \cdot \varepsilon_\beta$ для $\alpha, \beta \in S_5$ и тождеств

$$\alpha\beta(h) = \varepsilon_{\alpha\beta}h, \quad \alpha(\beta h) = \alpha(\varepsilon_\beta h) = \varepsilon_\beta(\alpha h) = \varepsilon_\beta \cdot \varepsilon_\alpha h.$$

Как известно, всякую перестановку можно представить в виде композиции транспозиций. Заметим, что $\varepsilon_{(ij)} = \pm 1$, так как $(ij) \cdot (ij)$ — тождественная перестановка.

Легко видеть, что для любых двух перестановок $(i'j')$ и (ij) выполняется тождество $(i'j') = (ii')(jj')(ij)(jj')(ii')$. Отсюда имеем, что $\varepsilon_{(ij)} = \varepsilon_{(i'j')}$. Поэтому, если расширение нетривиальное, то $\varepsilon_{(ij)} = -1$ для всех транспозиций $(ij) \in S_5$. Значит, ε_α совпадает со знаком $\varepsilon(\alpha)$ перестановки α для всех $\alpha \in S_5$.

Рассмотрим многочлен $\sqrt{D} = \prod_{i < j} (x_i - x_j)$. Выполняется тождество

$$\alpha\sqrt{D} = \varepsilon(\alpha)\sqrt{D}$$

для $\alpha \in S_5$.

Заметим, что

$$\alpha \frac{f}{\sqrt{D}} = \frac{\alpha f}{\alpha \sqrt{D}} = \frac{\varepsilon(\alpha) f}{\varepsilon(\alpha) \sqrt{D}} = \frac{f}{\sqrt{D}}.$$

Поэтому

$$\bar{f} = \frac{f}{\sqrt{D}} \in \mathbb{C}(\sigma_0, \sigma_1, \sigma_2, \sigma_3, \sigma_4),$$

значит, $K_0(f) = K_0(\bar{f}\sqrt{D}) = K_0(\sqrt{D})$. □

Далее понадобится еще

Лемма 31. *Поле*

$$K_1 = K_0(\sqrt{D}) \subset \mathbb{C}(x_1, x_2, \dots, x_5)$$

совпадает с множеством всех рациональных функций, не изменяющихся при четных перестановках переменных.

Доказательство. Проверим, что рациональная функция f не изменяется при четных перестановках переменных тогда и только тогда, когда она представляется в виде суммы симметрической функции f_1 и антисимметрической функции f_2 (т.е. такой, что $\alpha f = \varepsilon(\alpha) f$ для $\alpha \in S_5$). В одну сторону это очевидно.

Докажем обратное утверждение. В самом деле,

$$f = \frac{1}{2}(f + (12)f) + \frac{1}{2}(f - (12)f), \quad f_1 = \frac{1}{2}(f + (12)f), \quad f_2 = \frac{1}{2}(f - (12)f).$$

Проверим симметричность f_1 , т.е. равенство $\alpha f_1 = f_1$. Если α — четная, то $\alpha f_1 = \frac{1}{2}(\alpha f + \alpha(12)f) = \frac{1}{2}(f + (12)(12)\alpha(12)f)$, но перестановка $(12)\alpha(12)$ — четная, значит, $(12)\alpha(12)f = f$, откуда $\alpha f_1 = \frac{1}{2}(f + (12)f) = f_1$.

Аналогично проверяем равенство $\alpha f_2 = f_2$:

$$\alpha f_2 = \frac{1}{2}(\alpha f - \alpha(12)f) = \frac{1}{2}f - \frac{1}{2}((12)(12)\alpha(12)f) = \frac{1}{2}(f - (12)f) = f_2.$$

Если перестановка α — нечетная, то

$$\alpha f_1 = \frac{1}{2}(\alpha f + \alpha(12)f) = \frac{1}{2}((12)(12)\alpha f + \alpha(12)f) = \frac{1}{2}((12)f + f) = f_1,$$

т.к. перестановки $(12)\alpha$ и $\alpha(12)$ — четные. Кроме того,

$$\alpha f_2 = \frac{1}{2}(\alpha f - \alpha(12)f) = \frac{1}{2}((12)(12)\alpha f - \alpha(12)f) = -f_2.$$

Поэтому, если f — рациональная функция, не меняющаяся при четных перестановках, то $f = f_1 + f_2$, где f_1 — симметрическая, а f_2 — антисимметрическая функция.

Если f_2 — антисимметрическая функция, то $f_2 = \frac{f_2}{\sqrt{D}}\sqrt{D} = \bar{f}_2\sqrt{D}$, где $\bar{f}_2$ — симметрическая функция. Поэтому $f = f_1 + \bar{f}_2\sqrt{D}$, где f_1 и $\bar{f}_2$ — симметрические функции, и $f \in K_0(\sqrt{D}) = K_1$.

Обратно, если $f \in K_0(\sqrt{D}) = K_1$, то $f = f_1 + f_2\sqrt{D}$, где f_1 и f_2 — симметрические функции, значит, f не меняется при четных перестановках. $\square$

Нужны будут еще две леммы о перестановках.

Лемма 32. *Любая четная перестановка разлагается в произведение тройных циклов.*

Доказательство. Разложим четную перестановку в произведение четного числа транспозиций, разобьем это произведение на пары, а пары заменим на тройные циклы согласно тождеству

$$(i, j)(i', j') = (iji')(ji'j'). \quad \square$$

Лемма 33. *Если перестановка $(i_1, \dots, i_5)$ разложима, то справедливо тождество*

$$(i_1, i_2, i_3) = (i_4, i_3, i_1)(i_1, i_5)(i_2, i_4)(i_3, i_4)(i_1, i_5)(i_1, i_3, i_4).$$

Доказательство. Для доказательства достаточно проверить, что под действием произведения перестановок элементы передвигаются следующим образом:

$$\begin{aligned} i_1 &\rightarrow i_3 \rightarrow i_4 \rightarrow i_2, & i_2 &\rightarrow i_4 \rightarrow i_3, \\ i_3 &\rightarrow i_4 \rightarrow i_3 \rightarrow i_1, & i_4 &\rightarrow i_1 \rightarrow i_5 \rightarrow i_1 \rightarrow i_4. \end{aligned} \quad \square$$

Закончим доказательство теоремы. Пусть $K_2 = K_1(\sqrt[r]{a})$, $a \in K_1$, $r \geq 2$, и

$$\sqrt[r]{a} = f(x_1, x_2, x_3, x_4, x_5) \in \mathbb{C}(x_1, x_2, x_3, x_4, x_5).$$

Тогда для всякой перестановки $\alpha \in S_5$ имеет место равенство $\alpha f = \varepsilon_\alpha f$, где $\varepsilon_\alpha \in \sqrt[r]{a}$.

Заметим, что если $\{ij\} \cap \{i'j'\} = \emptyset$, то $\varepsilon_{(ij)(i'j')} = \pm 1$, так как $[(ij)(i'j')]^2$ — тождественная перестановка.

Применяя лемму 33 и учитывая, что

$$\varepsilon_{(i_4, i_3, i_1)} \cdot \varepsilon_{(i_1, i_3, i_4)} = \varepsilon_{(i_4, i_3, i_1)} \cdot \varepsilon_{(i_4, i_3, i_1)}^{-1} + 1,$$

имеем

$$\varepsilon_{(i_1, i_2, i_3)} = \varepsilon_{(i_4, i_3, i_1)} \varepsilon_{(i_1, i_3, i_4)} \varepsilon_{(i_1, i_5)(i_2, i_4)} \varepsilon_{(i_3, i_4)(i_1, i_5)},$$

откуда $\varepsilon_{(i_1 i_2 i_3)} = \pm 1$.

Однако $(i_1 i_2 i_3)^3$ — тождественная перестановка, значит, $\varepsilon_{(i_1 i_2 i_3)}^3 = \pm 1$. Поэтому $\varepsilon_{(i_1, i_2, i_3)} = 1$.

Из леммы 32 теперь следует, что $\varepsilon_\alpha = 1$ для всякой четной перестановки α .

Из леммы 31 тогда следует, что $K_2 = K_1(\sqrt[n]{a}) = K_1(f)$, $f \in K_1$, откуда $K_2 = K_1$. Повторяя эти рассуждения, получаем, что

$$K_1 = K_2 = K_3 = \dots = K_n.$$

Однако, согласно лемме 31, поле K_1 есть множество рациональных функций от $(x_1, x_2, x_3, x_4, x_5)$, не меняющихся при четных перестановках переменных, следовательно, оно не совпадает с полем всех рациональных функций $\mathbb{C}(x_1, x_2, x_3, x_4, x_5)$. Значит, искомая цепочка расширений невозможна. $\square$

Задачи и упражнения к § 4.20

1. Решите уравнение $x^5 - 5ax^3 + 5a^2x + a^5 + 1 = 0$.
2. С помощью замены переменных $x = u + v$ решите подобно кубическому уравнению уравнение $x^5 - 5ax^3 + 5a^2x - 2b = 0$.

Приложение. Образцы контрольных работ разных лет, экзаменационных вопросов и задач

Контрольная работа 1

1. Разложите на множители (с действительными коэффициентами) (i) $x^4 + 9$; (ii) $x^4 + 25$.
2. Докажите, что числа (i) $\sqrt{2} + \sqrt{3}$; (ii) $\sqrt{3} + \sqrt{5}$ — иррациональны.
3. Решите уравнения:
(i) $x^4 - 4x^3 - 2x^2 + 12x + 8 = 0$; (ii) $x^4 - 10x^3 + 4x^2 + 8 = 0$.
4. Докажите неравенства:
(i) $\frac{1}{2} \frac{3}{4} \frac{5}{6} \cdots \frac{2n-1}{2n} < \frac{1}{\sqrt{2n}}$; (ii) $\frac{1}{2} \frac{3}{4} \frac{5}{6} \cdots \frac{2n-1}{2n} > \frac{1}{2\sqrt{n}}$.

Контрольная работа 2

1. Найдите суммы: (i) $\sum_{k=1}^n k(3k+1)$; (ii) $\sum_{k=1}^n (k^2 + 2k - 1)$.
2. С помощью алгоритма Евклида найдите НОД чисел a и b и представьте его в виде $au + bv$, где u и v — целые: (i) $a = 24$, $b = 30$; (ii) $a = 36$, $b = 20$.
3. Найдите число и сумму всех натуральных делителей у чисел (i) 2772; (ii) 5940.
4. Вычислите значение функции Эйлера от чисел (i) 65; (ii) 72.
5. В разложениях (i) $(x + 1/x)^{12}$; (ii) $(x/3 - 3/x)^{12}$ найдите коэффициент при (i) x^8 ; (ii) x^4 .
6. Найдите суммы: (i) $C_n^0 + C_n^2 + \dots + C_n^{2k} + \dots$; (ii) $1 - C_n^1 + C_n^2 - C_n^3 + \dots$.

Контрольная работа 3

1. Найдите порядок подстановки π и определите ее знак:
(i) $\pi = \begin{pmatrix} 12345 \\ 24513 \end{pmatrix}$; (ii) $\pi = \begin{pmatrix} 123456 \\ 345612 \end{pmatrix}$.
2. В произвольной группе G определена новая операция

$$[f, g] = f^{-1} g^{-1} f g.$$

Докажите тождества: (i) $[f, g]^{-1} = [g, f]$, (ii) $f g [g, f] = f g$.

3. Решите уравнения:
(i) $x^4 - 5x^2 - 2x + 3 = 0$; (ii) $x^4 - 5x^2 + 2x + 3 = 0$.
4. Докажите для любых неотрицательных a и b неравенства:
(i) $a^3 + b^3 \geq ab(a+b)$; (ii) $(a^3 + b^3)(a+b) \geq (a^2 + b^2)^2$.
5. Докажите, что уравнение $x^3 - 3x + 1 = 0$ имеет три корня, и найдите сумму их (i) квадратов; (ii) кубов, а также уравнение, одним из корней которого является (i) сумма; (ii) произведение двух корней исходного уравнения.

6. Вычислите
- (i) $\sum_{k=1}^n k C_n^k$; (ii) $\sum_{k=1}^n (n-k) C_n^k$.
7. Найдите группу самосовмещений многочлена при перестановках переменных $(xz + yt)^2 + (xy - zt)^2$ и разложите его на множители.
8. Первенство интерната по футболу проводилось настолько нерегулярно, что в конце семестра выяснилось, что все команды сыграли разное число матчей. Докажите, что какие-то команды успели сыграть между собой более одного раза.

Вопросы к экзамену в 10-х классах (1999 год)

- Индукция и примеры ее применения. Формулы суммирования арифметической и геометрической прогрессий.
- Числа Фибоначчи. Формула Бине.
- Рекуррентные последовательности второго порядка.
- Простые числа. Бесконечность множества простых чисел. Наибольший общий делитель и наименьшее общее кратное.
- Алгоритм Евклида. Линейное представление наибольшего общего делителя. Леммы о делимости.
- Основная теорема арифметики.
- Перестановки и размещения.
- Перестановки с повторениями.
- Биномиальная теорема. Треугольник Паскаля. Тождество Паскаля.
- Биномиальная и полиномиальная теоремы.
- Сочетания с повторениями.
- Определение комплексных чисел. Операции над ними. Геометрическая интерпретация комплексных чисел.
- Многочлены и операции над ними. Деление с остатком.
- Схема Горнера. Теорема Безу. Теорема о числе корней у уравнений произвольной степени.
- Производные и кратные корни.
- Теорема Виета для уравнений произвольной степени.
- Алгоритм Евклида для многочленов. Линейное представление наибольшего общего делителя. Леммы о делимости многочленов. Понятие неприводимого многочлена.
- Однозначность разложения на множители многочленов над полем рациональных чисел.
- Операция сопряжения и свойства комплексных корней многочленов с действительными коэффициентами.
- Разложение на множители многочленов над полями действительных и комплексных чисел.
- Умножение и деление комплексных чисел в тригонометрической форме. Теоремы сложения для синуса и косинуса.
- Формулы Муавра и Эйлера. Формулы для синусов, косинусов и тангенсов кратных дуг.
- Извлечение корней n -й степени из комплексных чисел. Геометрическая интерпретация.
- Алгебраический метод извлечения квадратных корней из комплексных чисел. Решение квадратных уравнений в поле комплексных чисел.
- Группа корней n -й степени из единицы. Первообразные корни. Функция Эйлера и ее мультипликативное свойство. Формула Эйлера.

Образцы экзаменационных задач

1. Вычислите двумя способами $(1+i)^n$ и напишите соответствующие тождества с биномиальными коэффициентами.

2. Найдите число всех первообразных корней группы корней 1999-й степени из единицы.

3. Нарисуйте на комплексной плоскости множество точек z таких, что $\left| \frac{z-a}{1-\bar{a}z} \right| < 1$.

4. Найдите коэффициент при x^{10} у многочлена $(1+x+x^2)^{10}$.

5. Найдите сумму коэффициентов многочлена $(1-x+x^2)^{10}$.

6. Найдите сумму всех натуральных делителей числа 1999ⁿ.

7. Решите уравнение $(x^2+x+4)^2+8x(x^2+x+4)^2+15x=0$.

8. Решите уравнение $4(x+5)(x+6)(x+10)(x+12)-3x^2=0$.

9. Докажите, что

$$\cos x + \cos 3x + \dots + \cos(2n-1)x = \frac{\sin 2nx}{2 \sin x}.$$

10. Разложите на множители многочлен над полем действительных чисел: $2x^4 - x^3 - 9x^2 + 13x - 5$.

11. Разложите на множители многочлен над полем действительных чисел: $x^3 + 9x^2 + 11x - 21$.

12. Докажите, что

$$\sin x + \sin 3x + \dots + \sin(2n-1)x = \frac{\sin^2 nx}{\sin nx}.$$

13. Нарисуйте на комплексной плоскости множество точек z таких, что $\left| \frac{z-a}{z-b} \right| < 2$.

14. Разложите на множители многочлен над полем действительных чисел: $x^4 + 2x^3 - 16x^2 - 2x + 15$.

15. Решите уравнение $(x^2+x)^4=1$ в поле комплексных чисел.

16. Найдите $\max |z|$ при $|z+1/z|=a$.

17. Решите уравнение $x^6+1=0$.

18. Если окружность построена на отрезке $[i, -b/a + ic/a]$ как на диаметре, то она пересекает действительную ось в корнях уравнения $ax^2+bx+c=0$ и не пересекает ее, если это уравнение не имеет действительных корней.

19. Извлеките алгебраически корень пятой степени из единицы и постройте правильный пятиугольник циркулем и линейкой.

20. Хор состоит из 10 участников. Сколькими способами можно выбирать в течение трех дней по 6 участников хора так, чтобы каждый день были разные составы?

21. Школьник имеет 6 друзей и в течение 20 дней приглашает к себе трех из них так, что компания ни разу не повторяется. Сколькими способами он может это сделать?

22. В турпоход отправились 92 ученика. Бутерброды с колбасой взяли 47 учеников, с сыром — 38, с ветчиной — 42, и с сыром, и с колбасой — 28, и с колбасой, и с ветчиной — 26, и с сыром, и с ветчиной — 17. Все три вида бутербродов взяли 26 учеников, а несколько учеников взяли с собой пирожки. Сколько было последних?

23. Сколькими способами можно разделить 10 книг на 5 бандеролей по 2 в каждой?

24. Сколькими способами можно выбрать нечетное число предметов из данных 20?

25. Найдите средний член разложения $(1-x^2/2)^{14}$.

26. Найдите коэффициент при x^8 в разложении $(2+x-x^2)^5$.

27. Докажите, что

$$C_n^0 + C_n^3 + C_n^6 + \dots = \frac{1}{3} \left(2^n + 2 \cos \frac{\pi n}{3} \right).$$

28. Докажите, что

$$C_n^0 + C_n^4 + C_n^8 + \dots = \frac{1}{2} \left(2^{n-1} + 2^{n/2} \cos \frac{\pi n}{4} \right).$$

29. Найдите числа, сопряженные своему кубу.

30. Вычислите $\sqrt[4]{2 - i\sqrt{12}}$.

31. Вычислите $\sqrt[6]{\frac{1-i}{1+i\sqrt{3}}}$.

32. Выразите $\operatorname{tg} 6\varphi$ через $\operatorname{tg} \varphi$.

33. Выразите $\frac{\sin 6\varphi}{\sin \varphi}$ через $\cos \varphi$.

34. Представьте $\cos^6 x$ в виде линейной комбинации косинусов кратных дуг.

35. Докажите, что если $z + 1/z = 2 \cos x$, то $z^n + z^{-n} = 2 \cos nx$.

36. Решите уравнение $(x^3 - 3qx + p^3 - 3pq)^2 - 4(px + q)^3 = 0$.

37. Решите уравнение $x^3 - 3abx + a^3 + b^3 = 0$.

38. Составьте уравнение, корни которого равны кубам корней уравнения $x^3 + px + q = 0$.

39. Решите уравнение $ax^3 + bx^2 + cx + d = 0$, если его коэффициенты удовлетворяют условию $ad = bc$.

40. Решите уравнение $ax^3 + bx^2 + cx + d = 0$, если его коэффициенты составляют геометрическую прогрессию с данным знаменателем q .

41. Решите уравнение $x^3 + ax^2 + bx + c = 0$, если его коэффициенты удовлетворяют условию $ab = c$.

Предметный указатель

p -группа 97

Абе́ля—Руффини теорема 313

аксиома группы 71

алгоритм перевода из двоичной системы
в десятичную и обратно 157

аргумент комплексного числа 214

ассоциативность 71

Безу коэффициенты 15

— теорема 142, 276

Бине теорема 28

Брауэра А. теорема 162

Вьета теорема 184, 249

вложение 41

вычет n -й степени 110

— квадратичный 110

вычитание многочленов 135

Гаусса лемма 174

— теорема 13, 103, 106

гипербола 276

гомоморфизм 77, 88

граф 70

— полный 71

график отображения 40

группа 71

— абелева 77

— аддитивная кольца 101

— коммутативная 75, 77, 88, 283

— мультипликативная 284

— циклическая 76

группы изоморфные 76

гудерманиан 286

Данделена теорема 168

действительная часть 210

декартова степень 38

декремент перестановки 65

делимость многочленов 141

делитель 12

— многочленов наибольший общий
(НОД) 141

— наибольший общий (НОД) 13

— нуля 89

дерево степеней 163

детерминант 267

директриса 276

дискриминант 31

— кубического уравнения 239

— уравнения n -й степени 240

Диффи—Хеллмана система 131

дроби символические по модулю m 92

дробь непрерывная 20

— цепная 20

Дюпре теорема 29

Евклида алгоритм 20

— — обобщенный 23

— — расширенный 15

— алгоритм, обобщенный вариант 24

— теорема 12

Закон сокращения 91

знак перестановки 68

золотое сечение 27

Изоморфизм 76, 88

инверсия 66

индекс подгруппы 83

индекс элемента 109

Класс смежный левый 82

— — правый 82

— эквивалентности числа 282

ключ 119

кольцо 88

— без делителей нуля 90

— вычетов по модулю m 88

— гауссовых целых чисел 306

— целостное 90

корень 163

— из комплексного числа n -й степени
232

— кратный 31

— многочлена 142

— — кратности n 152

— — простой 152

— первообразный 103

— Энке 187

косинус гиперболический 225
 коэффициент биномиальный 47
 — полиномиальный 47
 кратное наименьшее общее 14
 криптоанализ 121
 криптография 119
 Кронекера алгоритм 176
 куб n -мерный k -ичный 38
 — — двоичный 38

Лагранжа теорема 83
 логарифм дискретный 109
 логарифмирование дискретное 131

Метод вилки 165
 — вычисления «цифра за цифрой» 165
 — Горнера 166
 — итерационный 166
 — Ньютона 166
 мнимая часть 210
 многочлен 134
 — антисимметрический 191
 — возвратный 180
 — интерполяционный Лагранжа 145
 — кососимметрический 191
 — круговой 230
 — неприводимый над полем 300
 — неприводимый над кольцом 173
 — нечетный 181
 — симметрический 183
 — — элементарный 183
 — тригонометрический 286
 — фундаментальный Лагранжа 144
 — Чебышёва 170
 — четный 181
 многочлены взаимные 180
 множество всех подмножеств 42
 — классов эквивалентности 282
 модуль комплексного числа 211
 мощность множества 39
 Муавра теорема 181
 — формула 216
 мультипликативность 118
 — функции Эйлера 96

Набор упорядоченный 38
 наложение 41
 норма 294
 — алгебраического числа 302

Область целостности 136
 образ множества 41
 объединение семейства множеств 40

— — одночлен 135, 138
 — старший 138
 операция обращения 61
 определитель 267
 остаток от деления 11
 — от деления многочленов 136
 Остроградского теорема 198
 отображение 40
 — взаимно однозначное 41
 — зашифрования 119
 — изоморфное 76
 — расшифрования 119
 отрезок фокальный 276

Парабола 276
 Паскаля тождество 47
 — треугольник 48
 перестановка маршрутная 120
 — обратная 61
 — с повторениями 46
 период 75
 — группы 84
 — — наименьший положительный 84
 — элемента наименьший
 положительный 75
 подграф 63
 подгруппа 70, 74
 — нормальная 84
 — собственная 74
 поле 90
 — деления круга 299
 — числовое 298
 полугруппа коммутативная 88
 порядок перестановки 67
 — элемента 75
 последовательность, обратная
 к последовательности Фибоначчи
 29
 построение циркулем и линейкой 311
 признаки неприводимости достаточные
 175
 принцип сложения 39
 произведение многочленов 135, 138
 — множеств декартово 38
 — перестановок 60
 — прямое групп 94
 — — операций 94
 — скалярное комплексных чисел 212
 производная многочлена 150
 пространство n -мерное арифметическое
 39
 — ключей 119

процесс итерационный 169

Разложение многочлена по степеням 152

разность множеств симметрическая 86

расширение пифагорово 308

— поля 299

— — квадратичное 299

— — простое 300

— радикальное 313

ребро графа 63, 71

резольвента Феррари 236, 242

результант 269

Самосовмещение графа 71

символ Золотарёва 114

— Якоби 115

символ Лежандра 110

синус гиперболический 225

система RSA 130

— вычетов полная 228

— симметрическая 186

— трапециевидная 265

— треугольная 265

слово 38

сложение комплексных чисел 210

сложность алгоритма 155

сочетание элементов 51

сочетания с повторениями 52

сравнение 84

сравнимость левая 84

— правая 84

степень многочлена 134, 138

— одночлена 138

сумма многочленов 134, 138

— множеств 96

суммой классов эквивалентности 283

считала 120

Таблица Энея 120

Тейлора теорема 153

теорема Виета 31

— Гаусса 174

тип перестановки циклический 65

тождество дистрибутивное 88

транспозиция 64

трансцендентные 271

Умножение комплексных чисел 210

Факторгруппа 87

факториал 45

— возрастающий 45

— убывающий 45

факторизация 178

— бесквадратная 196

Ферма теорема малая 90, 104

— — — для конечных полей 104

— теорема для групп малая 84

Фибоначчи числа 26

фокус гиперболы 276

— параболы 276

— эллипса 276

форма квадратичная 277

формула 72

— интерполяционная Ньютона 147

формулы Крамера 267

функция 40

— k -значной логики 43

— алгебры логики 43

— булева 43

— двузначной логики 43

— от n действительных переменных 43

— от n переменных 43

— полиномиальная 142

— Эйлера 79

Фурье теорема 167

Характеристика целостного кольца 101

Целая часть числа 28

цепочка аддитивная 160

цепь 54

цикл длины k 63

— порядка k 63

Частное комплексных чисел 211

— неполное 11

— от деления многочленов 136

Чебышёва многочлены первого

и второго рода 290

числа взаимно простые 13

— эквивалентные по модулю 282

число алгебраическое 173, 300, 302

— — над полем 300

— — целое 302

— иррациональное 28

— комплексное 210

— — сопряженное 211

— пифагорово 308

— простое 12

— — гауссово 306

— сопряженное алгебраическому 302

— составное 12

— целое 28

Шифр 119

— аффинный 120

— замены 119

— перестановки 119

Шифр Плейфера—Уитстона 127

шифр-система 119

шифрование 119

шифртекст 119

Эйлера критерий 110

— теорема 90, 96

Эйлера—Гаусса теорема 109

Эйнштейна признак 175

элемент единичный 71

— нейтральный 71

— обратимый 88

— обратный 71

— — многочлена 135

— примитивный 103

— простой 306

эллипс 276

Ядро Дирихле 294

— Фейера 295

Оглавление

Предисловие	3
Глава I. Числа и комбинаторика	4
§ 1.1. Позиционные системы счисления	4
§ 1.2. Натуральные числа	11
§ 1.3. Алгоритм Евклида и цепные дроби	20
§ 1.4. Числа Фибоначчи	27
§ 1.5. Квадратные уравнения	32
§ 1.6. Комбинаторика отображений	38
§ 1.7. Полиномиальная теорема	46
§ 1.8. Сочетания и разбиения	52
§ 1.9. Перестановки и подстановки	60
§ 1.10. Циклы и транспозиции	65
Глава II. Числа и группы	71
§ 2.1. Группа подстановок	71
§ 2.2. Группы и подгруппы	75
§ 2.3. Циклические группы	79
§ 2.4. Теорема Лагранжа	83
§ 2.5. Кольца и поля вычетов	88
§ 2.6. Прямое произведение	95
§ 2.7. Конечные поля	102
§ 2.8. Первообразные корни	107
§ 2.9. Алгебра и криптология	119
Глава III. Многочлены	135
§ 3.1. Кольцо многочленов	135
§ 3.2. Алгоритм Евклида и теорема Безу	142
§ 3.3. Интерполяция	145
§ 3.4. Производные и кратные корни	151
§ 3.5. Схема Горнера	155
§ 3.6. Аддитивные цепочки	161
§ 3.7. Приближенное вычисление корней многочленов	166
§ 3.8. Разложение на множители	174
§ 3.9. Взаимные многочлены	181
§ 3.10. Симметрические многочлены	184
§ 3.11. Быстрое умножение	192
§ 3.12. Разложение на бесквадратные множители	197

Глава IV. Алгебраические уравнения	204
§ 4.1. Решение кубических уравнений	204
§ 4.2. Неприводимый случай	208
§ 4.3. Комплексные числа	210
§ 4.4. Вычисления на калькуляторе	222
§ 4.5. Корни из комплексных чисел	227
§ 4.6. Кубические уравнения над полем комплексных чисел	233
§ 4.7. Уравнения четвертой степени	236
§ 4.8. Решение кубического уравнения методом Лагранжа	237
§ 4.9. Решение методом Лагранжа уравнений четвертой степени ..	241
§ 4.10. Решение методом Эйлера уравнений четвертой степени	245
§ 4.11. Основная теорема алгебры	248
§ 4.12. Как решать уравнения на экзаменах	254
§ 4.13. Системы уравнений	262
§ 4.14. Почему уравнения могут быть неограниченно трудными	272
§ 4.15. Алгебра и геометрия	276
§ 4.16. Комплексная тригонометрия	281
§ 4.17. Тригонометрические многочлены	287
§ 4.18. Расширения полей	298
§ 4.19. Построения циркулем и линейкой	308
§ 4.20. Теорема Абеля—Руффини	314
Приложение. Образцы контрольных работ разных лет, экза- менационных вопросов и задач	320
Предметный указатель	324